TCVN TIÊU CHUẨN QUỐC GIA

TCVN 8709-3:2011

ISO/IEC 15408-3:2008

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – CÁC TIÊU CHÍ ĐÁNH GIÁ AN TOÀN CNTT – PHẦN 3: CÁC THÀNH PHẦN ĐẢM BẢO AN TOÀN

Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security assurance components

HÀ NỘI – 2011

Mục lục

Lời nói đầu

TCVN 8709-3:2011 hoàn toàn tương đương ISO/IEC 15408-3:2008

TCVN 8709-3:2011 do Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Các thành phần đảm bảo an toàn như định nghĩa trong tiêu chuẩn này của TCVN 8709 là cơ sở cho các yêu cầu đảm bảo an toàn được biểu thị trong một Hồ sơ bảo vệ (PP) hoặc một Đích An toàn (ST).

Các yêu cầu này tạo thành một cách thức chuẩn để biểu thị các yêu cầu đảm bảo cho một Đích đánh giá (TOE). Phần này của tiêu chuẩn TCVN 8709 liệt kê danh mục các thành phần, các họ và lớp đảm bảo. Tiêu chuẩn TCVN 8709–3 cũng đồng thời xác định các tiêu chí đánh giá cho các PP và các ST, biểu thị các mức đảm bảo đánh giá dùng để xác định các thang bậc mà TCVN 8709 định trước cho việc đánh giá tính đảm bảo của các T, còn gọi là các Mức đảm bảo đánh giá (EAL).

Đối tượng của tiêu chuẩn này bao gồm các khách hàng, nhà phát triển và đánh giá viên cho các sản phẩm công nghệ thông tin (CNTT) an toàn. Tiêu chuẩn TCVN 8709–1 cung cấp thông tin bổ sung về các đối tượng mục tiêu của bộ tiêu chuẩn TCVN 8709, và về khả năng các nhóm đối tượng sử dụng TCVN 8709. Các nhóm này có thể gồm:

a) Các khách hàng, sử dụng phần này của TCVN 8709 khi chọn lựa các thành phần để biểu thị các yêu cầu đảm bảo nhằm thỏa mãn các mục tiêu an toàn đã biểu thị trong một PP hoặc ST, xác định các mức đảm bảo an toàn cho TOE theo yêu cầu.

b) Nhà phát triển, phản ánh lại thực tế hoặc nhận thức được các yêu cầu an toàn của khách hàng để thiết kế TOE, tham chiếu phần này của TCVN 8709 để diễn đạt các yêu cầu đảm bảo và xác định các phương thức đảm bảo cho các TOE.

c) Đánh giá viên, sử dụng các yêu cầu đảm bảo định nghĩa trong phần này của TCVN 8709 như một tuyên bố bắt buộc về các tiêu chí đánh giá khi xác định tính đảm bảo của các TOE và khi đánh giá các PP và các ST.

Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT –

Phần 3: Các thành phần đảm bảo an toàn

Information Technology – Security Techniques – Evaluation Criteria for IT –

Part 3: Security assurance components

1 Phạm vi áp dụng

Tiêu chuẩn này định nghĩa các yêu cầu đảm bảo cho bộ tiêu chuẩn. Tiêu chuẩn này gồm các mức đảm bảo đánh giá (EAL) dùng để xác định một cấp độ đo lường mức đảm bảo cho các TOE thành phần; các gói đảm bảo tổng hợp (CAP) dùng để xác định một cấp độ đo lường mức đảm bảo cho các TOE tổng hợp; các thành phần đảm bảo riêng biệt dùng cho việc tổng hợp các mức đảm bảo và các gói, và các tiêu chí đánh giá cho các PP và ST.

2 Tài liệu viện dẫn

Tài liệu viện dẫn sau đây không thể thiếu được khi áp dụng tài liệu tiêu chuẩn này:

TCVN 8709 – 1, *"Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 1: Giới thiệu và mô hình tổng quát"*.

TCVN 8709 – 2, *"Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 2: Các thành phần chức năng an toàn"*.

3 Thuật ngữ, định nghĩa, ký hiệu và các từ viết tắt

Các thuật ngữ, định nghĩa, ký hiệu và các từ viết tắt được nêu trong TCVN 8709-1.

4 Tổng quan

4.1 Bố cục của tiêu chuẩn

Điều 5 mô tả mô hình sử dụng trong các yêu cầu đảm bảo an toàn thuộc phần này của TCVN 8709.

Điều 6 mô tả cấu trúc trình bày của các lớp, họ, thành phần, các mức đảm bảo đánh giá trong mối quan hệ giữa chúng và cấu trúc của các gói đảm bảo tổng hợp, nêu đặc trưng các lớp và họ đảm bảo dùng trong các điều từ 9 đến điều 16.

Điều 7 cung cấp các định nghĩa chi tiết về các mức bảo đảm đánh giá (EAL).

Điều 8 cung cấp các định nghĩa chi tiết về các gói đảm bảo tổng hợp (CAP).

Điều 9 đến điều 16 cung cấp các định nghĩa chi tiết các lớp đảm bảo của tiêu chuẩn TCVN 8709-3.

Phụ lục A giải thích thêm và cung cấp các ví dụ về các khái niệm bên trong lớp phát triển.

Phụ lục B giải thích các khái niệm bên trong các đánh giá cho TOE tổng hợp và các lớp tổng hợp.

Phụ lục C tóm lược các liên thuộc giữa các thành phần đảm bảo.

Phụ lục D cung cấp một bảng tham chiếu chéo giữa các hồ sơ bảo vệ (PP) và các họ cũng như các thành phần của lớp APE.

Phụ lục E cung cấp một bảng tham chiếu chéo giữa các mức đảm bảo đánh giá (EAL) và các thành phần đảm bảo.

Phụ lục F cung cấp một bảng tham chiếu chéo giữa các gói đảm bảo tổng hợp (CAP) và các thành phần đảm bảo.

5 Mô hình đảm bảo

Mục đích của điều này là trình bày triết lý nền tảng của TCVN 8709 trong việc đảm bảo. Hiểu được điều này, độc giả sẽ hiểu được sở cứ của các yêu cầu đảm bảo trong TCVN 8709-3.

5.1 Triết lý của TCVN 8709

Triết lý TCVN 8709 thể hiện ở chỗ các nguy cơ mất an toàn và xâm hại cam kết chính sách an toàn của tổ chức cần được thể hiện rõ ràng và các biện pháp an toàn đã đề xuất cần biểu thị đầy đủ các mục đích dự kiến của chúng.

Mặt khác, các biện pháp cần được chọn để giảm thiểu khả năng điểm yếu, khả năng sử dụng một điểm yếu (ví dụ cố ý lợi dụng hoặc vô ý gây ra), và phạm vi thiệt hại có thể xảy ra từ việc một điểm yếu bị sử dụng. Ngoài ra, các biện pháp cần được chọn sao cho thuận tiện việc nhận diện tiếp tục các điểm yếu và giảm bớt, hạn chế và/hoặc thông báo về việc một điểm yếu đã bị lợi dụng hoặc bị khai thác.

5.2 Tiếp cận đảm bảo

Triết lý của bộ tiêu chuẩn là cung cấp sự đảm bảo dựa trên một phép đánh giá (kiểm tra một cách tích cực) sản phẩm CNTT để có thể đưa ra tính tin cậy. Đánh giá là phương thức truyền thống để bảo đảm và là cơ sở cho các tài liệu tiêu chí đánh giá trước đó. Tương tự với các phương thức đã có, TCVN 8709 kế thừa triết lý trước đó. TCVN 8709 đưa ra định mức giá trị pháp lý của văn bản và các sản phẩm CNTT bởi các chuyên gia đánh giá với mức nhấn mạnh tăng dần về phạm vi, mức chuyên sâu và tính chặt chẽ.

TCVN 8709 không loại trừ và cũng không diễn giải các đặc điểm liên quan của các phương thức đảm bảo khác. Nghiên cứu của TCVN 8709 tiếp tục theo hướng tìm các đường khác nhau để đạt được sự bảo đảm. Kết quả là những phương thức khác đạt được từ các hoạt động nghiên cứu sẽ được xem xét đưa vào TCVN 8709, và tiêu chuẩn này được cấu trúc để cho phép cập nhật thêm các phương thức mới.

5.2.1 Tầm quan trọng của các điểm yếu

Giả thiết rằng có các tác nhân đe dọa đang tích cực tìm kiếm cơ hội khai thác để xâm phạm các chính sách an toàn kể cả theo ý tốt và ý xấu, song đều là các hành động không an toàn. Các tác nhân đe dọa này có thể ngẫu nhiên lôi ra các điểm yếu an toàn, gây hại cho tổ chức. Do nhu cầu xử lý các thông tin nhạy cảm và do thiếu các sản phẩm đủ tin cậy, luôn tồn tại rủi ro do lỗi của CNTT. Nghĩa là, các lỗ hổng an toàn CNTT có thể dẫn đến mất mát đáng kể.

Các lỗ hổng an toàn CNTT xuất hiện thông qua việc khai thác có chủ ý hoặc vô tình làm phát sinh các điểm yếu khi ứng dụng CNTT vào hoạt động liên quan.

Cần có các bước thực hiện nhằm chống lại các điểm yếu phát sinh trong các sản phẩm CNTT. Trong các bước này, các điểm yếu cần được:

a) loại bỏ - nghĩa là cần có các bước thực hiện tích cực nhằm vạch rõ, xóa bỏ hoặc vô hiệu hóa mọi điểm yếu có tác dụng;

b) giảm thiểu – nghĩa là cần có các bước thực hiện tích cực nhằm giảm bớt, đến một mức độ chấp nhận được, ảnh hưởng có thể khi một điểm yếu bất kỳ được khai thác;

c) theo dõi - nghĩa là cần có các bước thực hiện tích cực nhằm đảm bảo mọi cố gắng khai thác một điểm yếu hiện hữu sẽ bị phát hiện và thiệt hại gây ra bị hạn chế;

5.2.2 Nguyên nhân của các điểm yếu

Các điểm yếu có thể nảy sinh qua các lỗi trong:

a) các yêu cầu – nghĩa là, một sản phẩm CNTT có thể có mọi chức năng và đặc trưng theo yêu cầu đối với chúng , song luôn chứa các điểm yếu thể hiện chúng không phù hợp hoặc không hiệu quả về góc độ an toàn;

b) phát triển - nghĩa là, một sản phẩm CNTT không đáp ứng các đặc tả và các điểm yếu nảy sinh là kết quả của các chuẩn phát triển không đủ hoặc lựa chọn thiết kế không phù hợp;

c) khai thác - nghĩa là, một sản phẩm CNTT đã được thiết kế phù hợp cho một đặc tả đúng song các điểm yếu có thể nảy sinh là kết quả của việc kiểm soát hoạt động không phù hợp.

5.2.3 Đảm bảo trong bộ TCVN 8709

Đảm bảo là cơ sở cho tính tin cậy mà một sản phẩm CNTT cần thỏa mãn các mục tiêu an toàn của chúng. Đảm bảo có thể nhận được từ tham chiếu tới các nguồn như các xác nhận không có minh chứng, kinh nghiệm liên quan trước đó, hoặc kinh nghiệm xác định nào đó. Tuy nhiên, TCVN 8709 cung cấp sự đảm bảo thông qua điều tra tích cực. Điều tra tích cực là một cách đánh giá các sản phẩm CNTT nhằm xác định các đặc tính an toàn của chúng.

5.2.4 Đảm bảo thông qua đánh giá

Đánh giá là phương thức truyền thống để đạt được sự đảm bảo, và là cơ sở của phương pháp TCVN 8709. Các kỹ thuật đánh giá có thể bao gồm song không hạn chế các nội dung sau:

a) Phân tích và kiểm tra các tiến trình và các thủ tục;

b) Kiểm tra hiện trạng áp dụng các tiến trình và các thủ tục;

c) Phân tích tính tương hợp giữa các mô tả thiết kế TOE;

d) Phân tích mô tả thiết kế TOE so với các yêu cầu;

e) Kiểm tra các bằng chứng;

f) Phân tích các tài liệu hướng dẫn;

g) Phân tích các phép do kiểm tra chức năng đã thiết lập và các kết quả đạt được;

h) Kiểm thử chức năng độc lập;

i) Phân tích các điểm yếu (bao gồm các giả thiết về khiếm khuyết);

j) Kiểm thử độ thẩm thấu;

5.3 Cấp độ đảm bảo đánh giá của bộ TCVN 8709

Triết lý của TCVN 8709 xác nhận rằng khi có nhiều nỗ lực đánh giá hơn thì sẽ đạt được các kết quả bảo đảm hơn, đích đặt ra là áp dụng nỗ lực tối thiểu theo yêu cầu để đưa ra mức độ đảm bảo cần thiết. Mức độ tăng dần các nỗ lực dựa vào:

a) Phạm vi – nghĩa là nỗ lực nhiều hơn do một phần lớn hơn của sản phẩm CNTT được xem xét;

b) Chuyên sâu – nghĩa là nỗ lực nhiều hơn do cần triển khai một mức thiết kế và triển khai chi tiết hơn;

c) Chặt chẽ - nghĩa là nỗ lực nhiều hơn do phải áp dụng theo một phương thức bắt buộc có cấu trúc hơn.

6 Các thành phần đảm bảo an toàn

6.1 Cấu trúc các lớp, họ và thành phần đảm bảo an toàn

Các điều khoản con sau đây mô tả các kết cấu sử dụng để biểu thị các lớp, thành phần và các họ đảm bảo.

Hình 1 trình bày các yêu cầu đảm bảo (SAR) được xác định trong tiêu chuẩn này (TCVN 8709 – 3). Lưu ý rằng tập hợp trừu tượng nhất của các yêu cầu đảm bảo SAR được coi là một lớp. Mỗi lớp chứa các họ đảm bảo, mỗi họ lại chứa các thành phần đảm bảo, còn thành phần thì chứa các phần tử đảm bảo. Các lớp và các họ được dùng để cung cấp một tập hợp phân loại các yêu cầu đảm bảo, còn các thành phần dùng để đặc tả các yêu cầu đảm bảo SAR trong một PP/ST.

6.1.1 Cấu trúc lớp đảm bảo

Hình 1 biểu diễn cấu trúc lớp đảm bảo.

6.1.1.1 Tên lớp

Mỗi lớp đảm bảo được gán một tên duy nhất. Tên biểu thị các chủ đề nêu trong lớp đảm bảo.

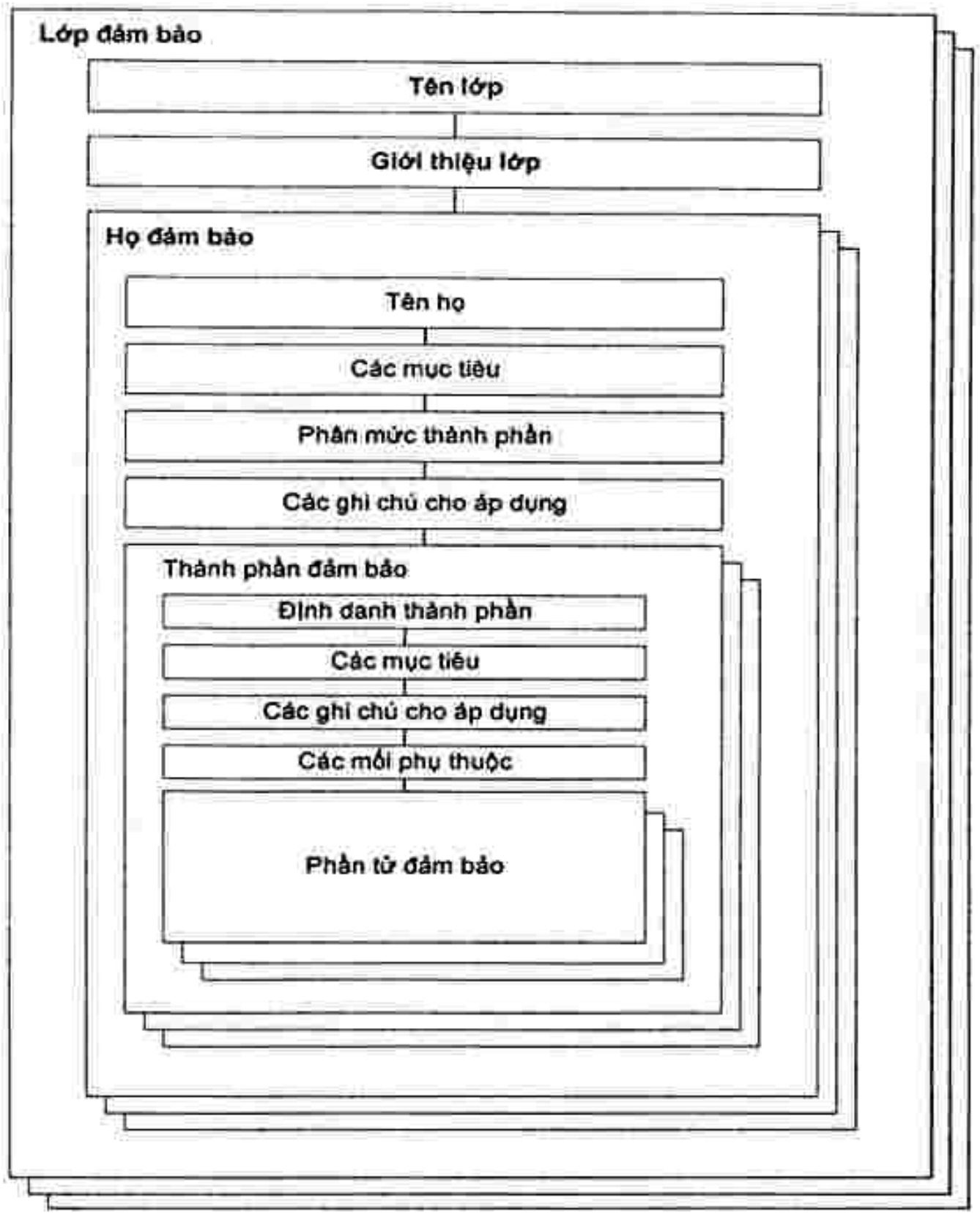
Một dạng viết tắt thống nhất cho tên lớp đảm bảo cũng được cung cấp. Đây là phương thức cơ bản để tham chiếu tới lớp đảm bảo. Quy ước đặt ra là một chữ "A" nối tiếp bởi 2 chữ cái biểu thị tên lớp.

6.1.1.2 Giới thiệu lớp

Mỗi lớp đảm bảo có một điều khoản nhỏ giới thiệu nhằm mô tả tập hợp của lớp và chứa thông tin hỗ trợ về mục đích của lớp.

6.1.1.3 Các họ đảm bảo

Mỗi lớp đảm bảo chứa ít nhất một họ đảm bảo. Cấu trúc của các họ đảm bảo được mô tả trong điều khoản sau đây.



Hình 1 – Phân cấp lớp/họ/thành phần/phần tử đảm bảo

6.1.2 Cấu trúc họ đảm bảo

Hình 1 mô tả cấu trúc họ đảm bảo.

6.1.2.1 Tên họ

Mỗi họ đảm bảo được gán một tên duy nhất. Tên cung cấp thông tin mô tả về các chủ đề nêu trong họ đảm bảo. Mỗi họ đảm bảo được đặt trong lớp đảm bảo có chứa các họ khác với cùng mục đích.

Một dạng viết tắt thống nhất cho tên họ đảm bảo cũng được cung cấp. Đây là phương thức cơ bản để tham chiếu tới họ đảm bảo. Quy ước đặt ra là sử dụng dạng viết tắt của tên lớp nối tiếp bởi một gạch dưới, tiếp đó là 3 chữ cái biểu thị tên họ.

6.1.2.2 Các mục tiêu

Điều khoản các mục tiêu của họ đảm bảo biểu thị mục đích của họ đảm bảo.

Điều khoản này mô tả các mục tiêu, cụ thể là các mục tiêu liên quan trong mô hình đảm bảo của TCVN 8709 mà họ này sẽ đề cập đến. Việc mô tả cho một họ đảm bảo được duy trì ở một mức tổng quát. Mọi chi tiết đặc trưng theo yêu cầu của các mục tiêu được kết hợp trong một thành phần đảm bảo riêng.

6.1.2.3 Phân mức thành phần

Mỗi họ đảm bảo chứa một hoặc nhiều thành phần đảm bảo. Điều khoản này của họ đảm bảo mô tả các thành phần sẵn có và giải thích sự khác biệt giữa chúng. Mục đích chính của chúng là nhằm phân biệt giữa các thành phần đảm bảo một khi đã xác định rằng họ đảm bảo là một phần hữu ích và cần thiết cho các yêu cầu đảm bảo (SAR) của một PP/ST.

Các họ đảm bảo chứa nhiều hơn một thành phần được phân mức và sở cứ được cung cấp về việc phân mức các thành phần như thế nào. Sở cứ này gồm phạm vi, chiều sâu và/hoặc tính chặt chẽ.

6.1.2.4 Chú thích ứng dụng

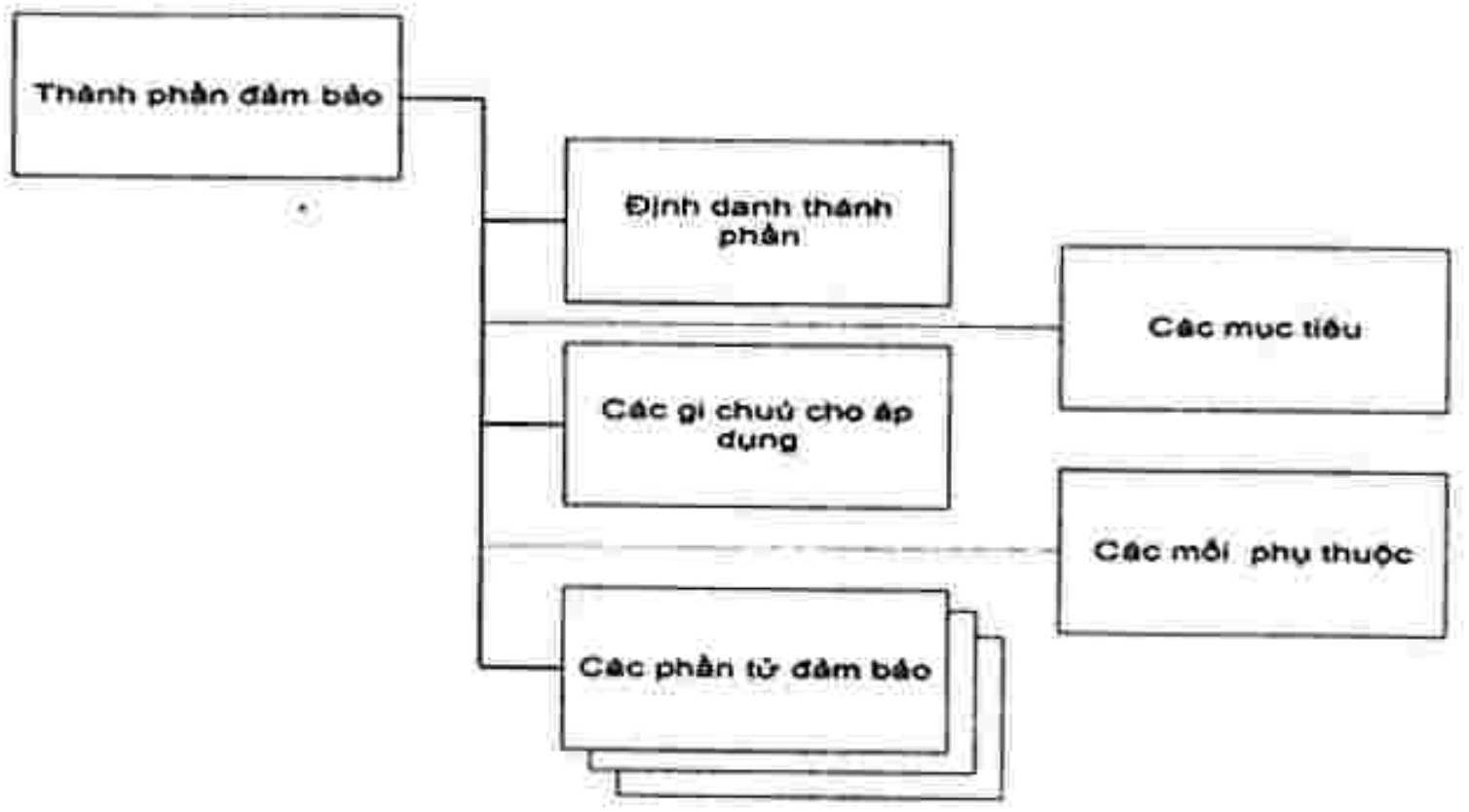
Điều khoản về chú thích ứng dụng của họ đảm bảo, nếu có, sẽ chứa thông tin bổ trợ thêm cho họ đảm bảo. Thông tin này cần thể hiện sự quan tâm cụ thể cho những người sử dụng họ đảm bảo (ví dụ các chủ thể PP hoặc ST, các nhà thiết kế TOE, những đánh giá viên). Việc biểu diễn thông tin là không bắt buộc và bao gồm, ví dụ như các cảnh báo về giới hạn và phạm vi sử dụng, trong đó cần có những lưu ý đặc biệt.

6.1.2.5 Các thành phần đảm bảo

Mỗi họ đảm bảo có ít nhất một thành phần đảm bảo. Cấu trúc của các thành phần đảm bảo được cung cấp ở điều khoản con sau đây.

6.1.3 Cấu trúc thành phần đảm bảo

Hình 2 biểu diễn cấu trúc thành phần đảm bảo.



Hình 2 – Cấu trúc thành phần đảm bảo

Mối quan hệ giữa các thành phần trong một họ được nhấn mạnh qua quy ước viết đậm. Các phần này của các yêu cầu là mới, cải tiến hoặc hiệu chỉnh theo các yêu cầu của thành phần trước đó trong phân lớp cấu trúc đã nhấn mạnh.

6.1.3.1 Định danh thành phần

Điều khoản định danh thành phần cung cấp các thông tin mô tả cần thiết để định danh, phân nhóm, đăng ký và tham chiếu cho một thành phần.

Mỗi thành phần đảm bảo được gán một tên duy nhất. Tên cung cấp thông tin mô tả về các chủ đề nêu trong thành phần đảm bảo. Mỗi thành phần đảm bảo được đặt trong họ đảm bảo có chia sẻ mục tiêu an toàn của chúng.

Một dạng viết tắt thống nhất cho tên thành phần đảm bảo cũng được cung cấp. Đây là phương thức cơ bản để tham chiếu tới thành phần đảm bảo. Quy ước đặt ra là sử dụng dạng viết tắt của tên họ nối tiếp bởi một thời kỳ và tiếp đó là một ký tự số. Các ký tự số cho các thành phần bên trong một họ được gán tuần tự, bắt đầu từ 1.

6.1.3.2 Các mục tiêu

Điều khoản các mục tiêu của thành phần đảm bảo, nếu có, sẽ chứa các mục tiêu đặc trưng cho thành phần đảm bảo cụ thể. Đối với các thành phần đảm bảo có điều khoản con này, điều khoản sẽ biểu thị mục đích đặc trưng của thành phần và giải thích chi tiết về các mục tiêu.

6.1.3.3 Chú thích ứng dụng

Điều khoản về chú thích ứng dụng của thành phần đảm bảo, nếu có, sẽ chứa thông tin bổ trợ thêm cho phép sử dụng thành phần.

6.1.3.4 Các mối phụ thuộc

Các mối phụ thuộc giữa các thành phần đảm bảo nảy sinh khi một thành phần không tự nó tồn tại mà phải dựa trên sự hiện diện của thành phần khác.

Mỗi thành phần đảm bảo cung cấp một danh sách đầy đủ các mối phụ thuộc với các thành phần đảm bảo khác. Một vài thành phần có thể liệt kê "không phụ thuộc" để chỉ ra sự không phụ thuộc. Các thành phần phụ thuộc nêu trên có thể có các mối phụ thuộc trong các thành phần khác.

Danh sách phụ thuộc xác định ra tập tối thiểu các thành phần đảm bảo mà chúng dựa vào. Các thành phần được phân cấp theo thành phần trong danh sách phụ thuộc có thể được dùng để thỏa mãn tính phụ thuộc.

Trong một số trường hợp đặc biệt, tính phụ thuộc đã biểu thị có thể không áp dụng được. Chủ thể PP/ST có thể tùy chọn không thỏa mãn tính phụ thuộc này thông qua việc cung cấp sở cứ tại sao các mối phụ thuộc đã cho không áp dụng được.

6.1.3.5 Các thành phần đảm bảo

Một tập các thành phần đảm bảo được cung cấp cho mỗi thành phần đảm bảo. Một phần tử đảm bảo là một yêu cầu an toàn và nếu tiếp tục chia nhỏ, sẽ không cho một kết quả đánh giá có nghĩa. Đó là yêu cầu an toàn nhỏ nhất chấp nhận được trong TCVN 8709.

Mỗi thành phần đảm bảo được xác định là thuộc một trong 3 tập các phần tử đảm bảo sau đây:

a) Phần tử hành động của nhà phát triển: Là các hành động cần được thực thi bởi nhà phát triển. Tập các hành động này tiếp tục được nêu rõ trong tài liệu chứng cứ được tham chiếu trong tập các phần tử sau đây. Các yêu cầu cho các hành động của nhà phát triển được xác định bởi việc thêm chữ cái "D" vào số hiệu phần tử.

b) Nội dung và biểu diễn của các phần tử chứng cứ: là chứng cứ yêu cầu, nghĩa là chứng cứ cần biểu thị gì, thông tin nào cần có trong chứng cứ. Các yêu cầu về nội dung và biểu diễn chứng cứ được xác định bởi việc thêm chữ cái "C" vào số hiệu phần tử.

c) Các phần tử hành động của đánh giá viên: Là các hành động cần được thực thi bởi đánh giá viên. Tập các hành động chứa sự khẳng định rõ ràng về sự thỏa mãn các yêu cầu đã mô tả trước đó trong Các phần tử nội dung và trình bày. Nó cũng chứa các hành động và phân tích rõ ràng cần thực hiện bổ sung thêm cho những gì nhà phát triển đã làm. Các hành động đánh giá ngầm định cũng được thực hiện như là kết quả của các phần tử hành động của nhà phát triển do các hành động này không chứa trong nội dung và biểu diễn của các phần tử chứng cứ. Các

yêu cầu về hành động của đánh giá viên được xác định bởi việc thêm chữ cái "E" vào số hiệu phần tử.

Các hành động của nhà phát triển, nội dung và biểu diễn chứng cứ xác định các yêu cầu đảm bảo được dùng để biểu thị trách nhiệm của nhà phát triển trong việc biểu diễn sự đảm bảo khi đích đánh giá (TOE) thỏa mãn các yêu cầu đảm bảo cho một PP hoặc một ST.

Các hành động của đánh giá viên xác định trách nhiệm của đánh giá viên ở 2 khía cạnh đánh giá. Khía cạnh thứ nhất là tính hợp lệ của PP/ST, trong tương quan với các lớp APE và ASE trong các điều khoản APE: Đánh giá hồ sơ bảo vệ và ASE: Đánh giá đích an toàn. Khía cạnh thứ 2 là kiểm chứng tính tuân thủ của các TOE với các yêu cầu chức năng (SFR) và yêu cầu đảm bảo (SAR) của chúng. Qua việc biểu thị PP/ST hợp lệ và các yêu cầu thỏa mãn bởi TOE, đánh giá viên có thể cung cấp một cơ sở tin cậy rằng TOE giải quyết vấn đề bảo mật đã được đặt ra trong môi trường xử lý của nó.

Phần tử hành động của nhà phát triển, Các phần tử nội dung và trình bày, và các phần tử hành động rõ ràng của đánh giá viên sẽ xác định nỗ lực của đánh giá viên cần sử dụng để kiểm chứng các đòi hỏi an toàn tạo ra trong ST của TOE.

6.1.4 Các phần tử đảm bảo

Mỗi phần tử biểu thị một yêu cầu cần thỏa mãn. Các công bố yêu cầu này cần rõ ràng, chính xác và không mập mờ. Bởi vậy, chúng không có các câu phức hợp: mỗi yêu cầu riêng biệt được công bố là một phần tử riêng.

6.1.5 Danh mục các thành phần

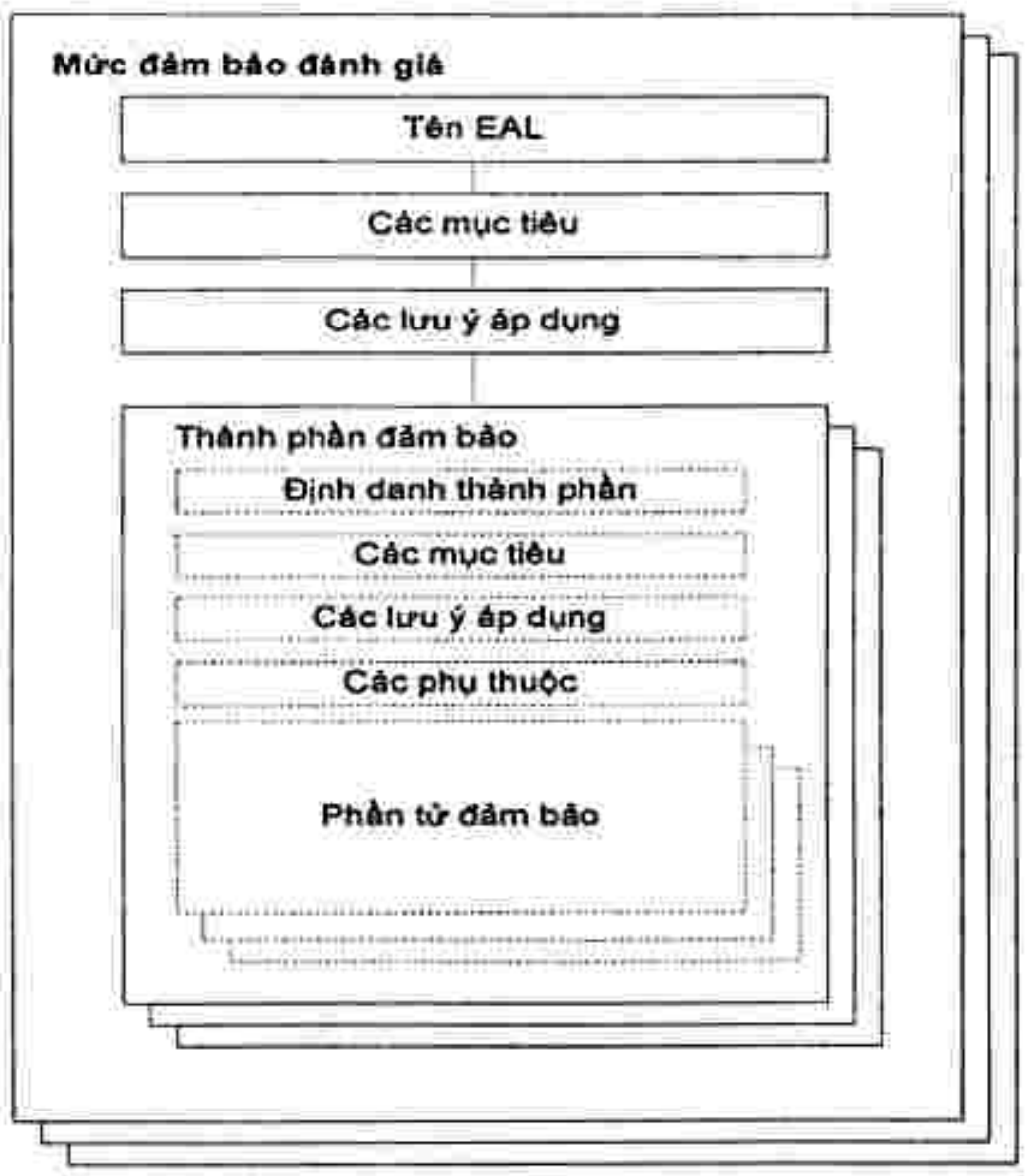
Trong phần này của TCVN 8709 chứa các lớp của các họ và các thành phần, chúng được phân nhóm dựa trên cơ sở của các đảm bảo liên quan. Tại điểm bắt đầu của mỗi lớp là một đồ thị thông tin về các họ trong lớp và các thành phần trong mỗi họ.

Hình 3 – Ví dụ về sơ đồ phân cấp lớp

Trong hình 3 ở trên, lớp được thể hiện với một họ duy nhất. Họ này chứa 3 thành phần theo kiến trúc tuyến tính (nghĩa là thành phần 2 đòi hỏi nhiều hơn thành phần 1 với các biểu thức về hành động đặc trưng, chứng cứ đặc trưng, hoặc tính chặt chẽ của các hành động hoặc chứng cứ). Các họ đảm bảo trong phần này của TCVN 8709 đều thuộc phân lớp tuyến tính, mặc dù tính tuyến tính không phải là tiêu chí bắt buộc cho các họ đảm bảo có thể bổ sung thêm trong tương lai.

6.2 Cấu trúc EAL

Hình 4 trình bày các EAL và cấu trúc liên quan định nghĩa trong tiêu chuẩn này. Lưu ý rằng trong khi hình chỉ ra các nội dung của các thành phần đảm bảo, thông tin này dự kiến sẽ đưa vào trong một EAL qua tham chiếu tới các thành phần thực tế được định nghĩa trong TCVN 8709.



Hình 4 - Cấu trúc EAL

6.2.1 Tên EAL

Mỗi EAL được gán một tên duy nhất. Tên cung cấp thông tin mô tả về nội dung của EAL.

Một dạng viết tắt thống nhất cho tên EAL cũng được cung cấp. Đây là phương thức cơ bản để tham chiếu tới EAL.

6.2.2 Mục tiêu

Điều khoản mục tiêu của EAL biểu thị mục đích của EAL.

6.2.3 Chú thích ứng dụng

Điều khoản về chú thích ứng dụng của EAL, nếu có, sẽ chứa thông tin thể hiện sự quan tâm cụ thể cho những người sử dụng EAL (ví dụ các chủ thể PP hoặc ST, các nhà thiết kế TOE với mục tiêu hướng tới EAL này, các đánh giá viên). Việc biểu diễn thông tin là không bắt buộc và bao gồm, ví dụ như các cảnh báo về giới hạn và phạm vi sử dụng, trong đó cần có những lưu ý đặc biệt.

6.2.4 Các thành phần đảm bảo

Một tập các thành phần đảm bảo đã được chọn cho mỗi EAL.

Một mức cao của đảm bảo hơn mức được cung cấp bởi một EAL cho trước có thể đạt được qua:

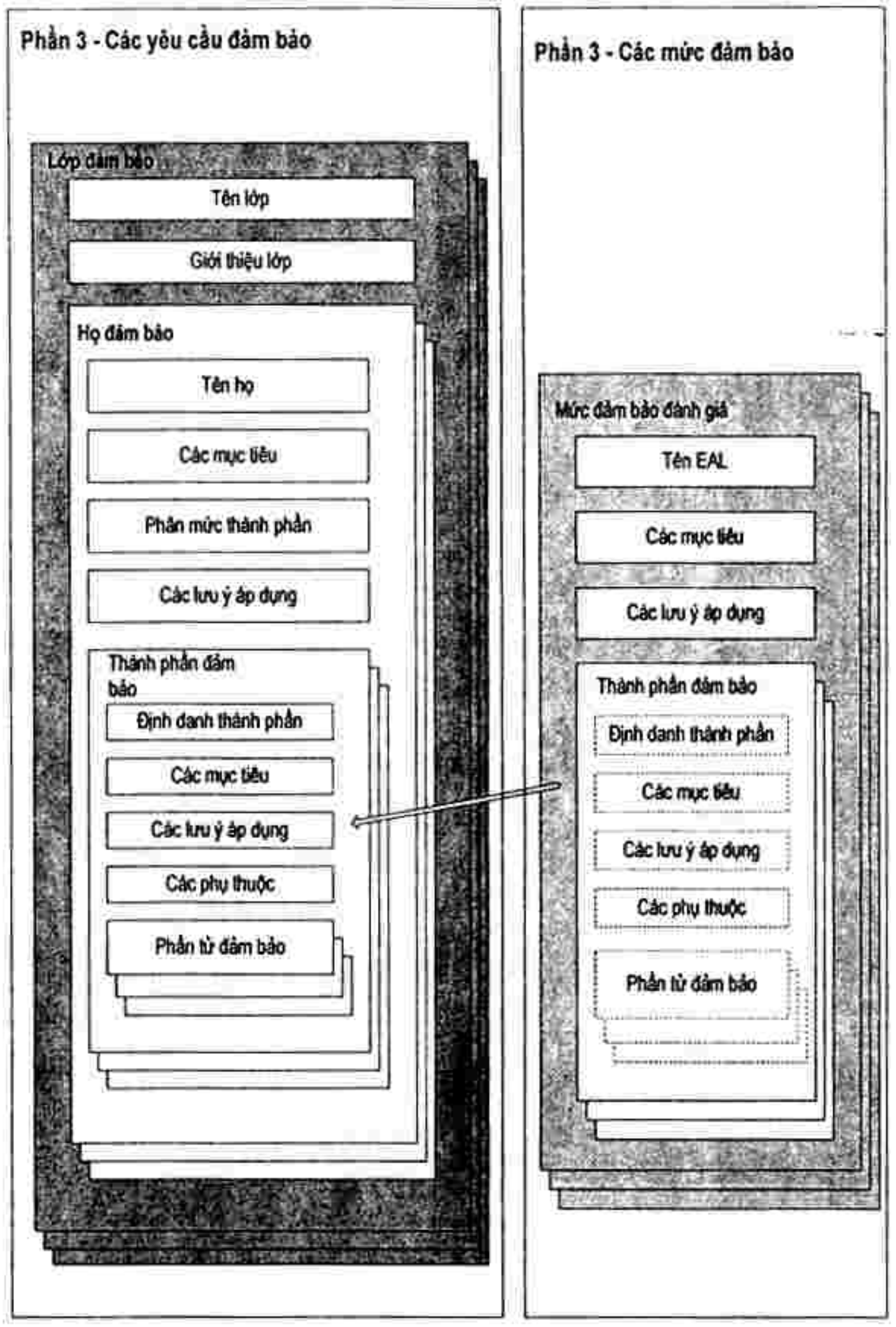
a) chứa các thành phần đảm bảo bổ sung từ các họ đảm bảo khác hoặc

b) thay thế một thành phần đảm bảo với một thành phần đảm bảo mức cao hơn từ cùng một họ đảm bảo.

6.2.5 Mối quan hệ giữa đảm bảo và các mức đảm bảo

Hình 5 trình bày mối quan hệ giữa các yêu cầu đảm bảo (SAR) và các mức đảm bảo xác định trong TCVN 8709. Trong khi các thành phần đảm bảo tiếp tục phân tách ra thành các phần tử đảm bảo, các

phần tử đảm bảo khong thể tham chiếu riêng biệt bởi các mức đảm bảo. Lưu ý rằng mũi tên ở trong hình biểu thị tham chiếu từ một EAL đến một thành phần đảm bảo bên trong lớp nơi nó được xác định.

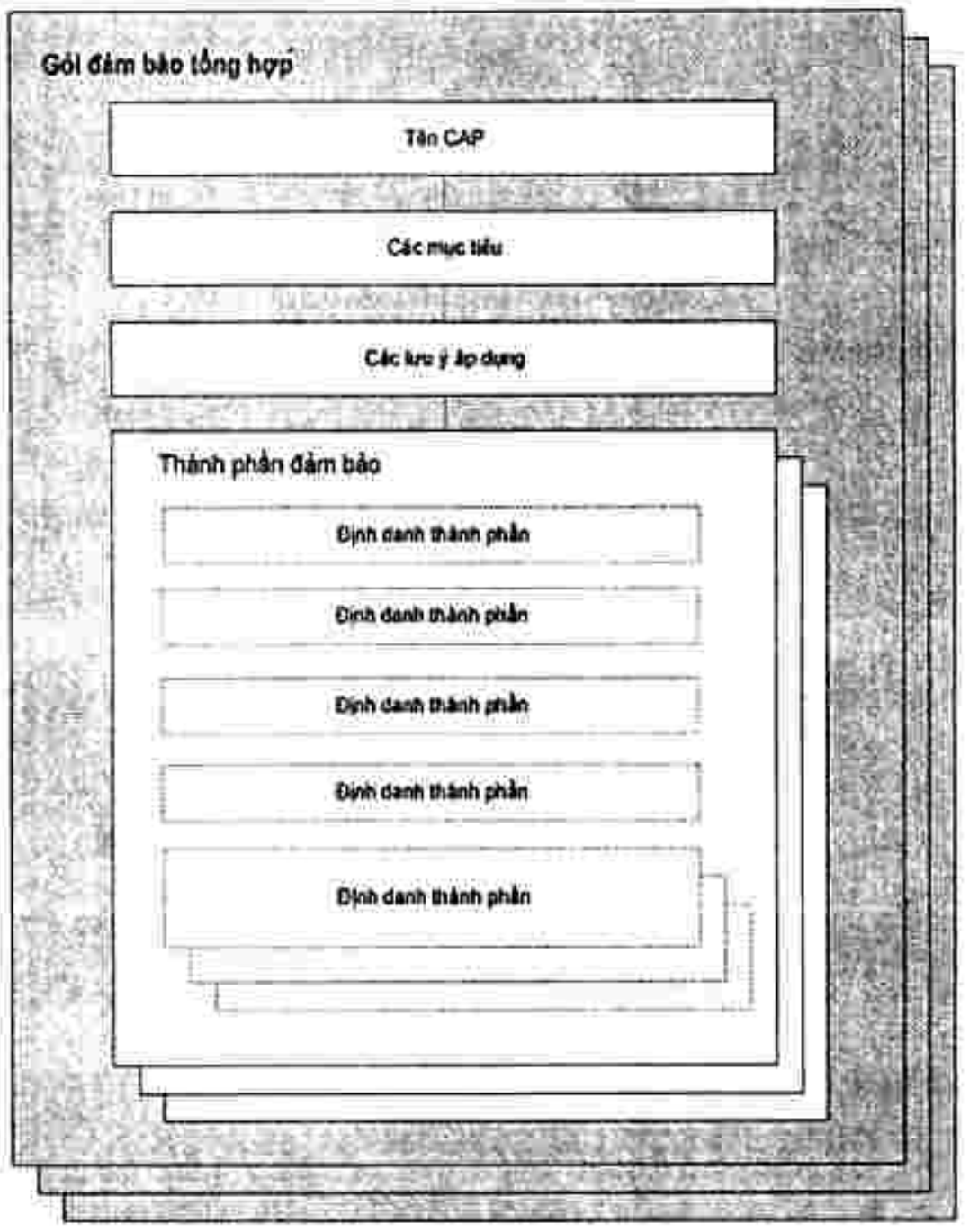


Hình 5 – Quan hệ giữa đảm bảo và mức đảm bảo

6.3 Cấu trúc CAP

Cấu trúc của gói đảm bảo tổng hợp (CAP) tương tự như của các mức đảm bảo đánh giá (EAL). Khác nhau chính giữa chúng là kiểu của đích đánh giá (TOE) mà chúng áp dụng; các EAL áp dụng cho thành phần của TOE còn CAP áp dụng cho các đích đánh giá tổng hợp.

Hình 6 trình bày các gói đảm bảo tổng hợp (CAP) và cấu trúc kết hợp được định nghĩa trong TCVN 8709-3. Lưu ý rằng trong khi hình chỉ ra các nội dung của các thành phần đảm bảo, thông tin này dự kiến sẽ đưa vào trong một CAP qua tham chiếu tới các thành phần thực tế định nghĩa trong TCVN 8709.



Hình 6 – Cấu trúc CAP

6.3.1 Tên CAP

Mỗi CAP được gán một tên duy nhất. Tên cung cấp thông tin mô tả về nội dung của CAP.

Một dạng viết tắt thống nhất cho tên CAP cũng được cung cấp. Đây là phương thức cơ bản để tham chiếu tới CAP.

6.3.2 Mục tiêu

Điều khoản mục tiêu của CAP biểu thị mục đích của CAP.

6.3.3 Chú thích ứng dụng

Điều khoản về chú thích ứng dụng của CAP, nếu có, sẽ chứa thông tin thể hiện sự quan tâm cụ thể cho những người sử dụng CAP (ví dụ các chủ thể PP hoặc ST, những người hợp nhất các TOE tổng hợp với mục tiêu hướng tới CAP này, các đánh giá viên). Việc biểu diễn thông tin là không bắt buộc và bao gồm, ví dụ như các cảnh báo về giới hạn và phạm vi sử dụng, trong đó cần có những lưu ý đặc biệt.

6.3.4 Các thành phần đảm bảo

Một tập các thành phần đảm bảo đã được chọn cho mỗi CAP.

Một vài các mối phụ thuộc nhận dạng các hoạt động diễn ra trong khi đánh giá các thành phần phụ thuộc dựa vào hoạt động của TOE tổng hợp. Nếu không nhận dạng rõ ràng được các mối phụ thuộc trong hoạt động của thành phần phụ thuộc thì các mối phụ thuộc sẽ là một cách đánh giá khác của TOE tổng hợp.

Một mức cao của đảm bảo hơn mức được cung cấp bởi CAP cho trước có thể đạt được qua:

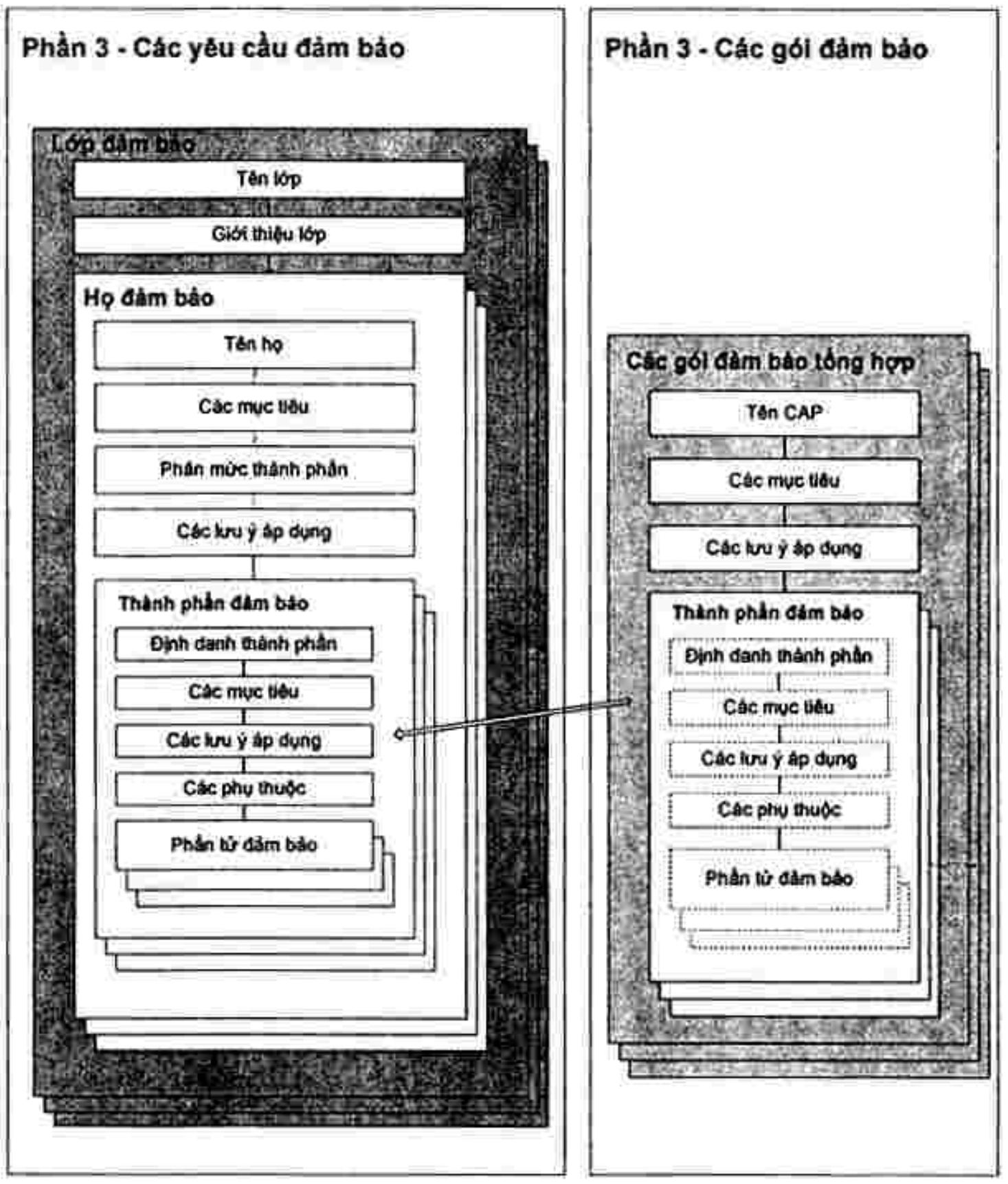
a) chứa các thành phần đảm bảo bổ sung từ các họ đảm bảo khác hoặc

b) thay thế một thành phần đảm bảo với một thành phần đảm bảo mức cao hơn từ cùng một họ đảm bảo.

Các thành phần kết cấu trong các gói đảm bảo CAP không nên sử dụng làm phần mở rộng cho các đánh giá thành phần TOE vì nó có thể cung cấp sự đảm bảo không đầy đủ cho những thành phần đó.

6.3.5 Mối quan hệ giữa đảm bảo và các mức đảm bảo

Hình 7 trình bày mối quan hệ giữa các yêu cầu đảm bảo (SAR) và các gói đảm bảo tổng hợp định nghĩa trong TCVN 8709. Trong khi các thành phần đảm bảo tiếp tục phân tách ra thành các phần tử đảm bảo, các phần tử đảm bảo không thể tham chiếu riêng biệt bởi các gói đảm bảo. Lưu ý rằng mũi tên ở trong hình biểu thị tham chiếu từ CAP đến một thành phần đảm bảo bên trong lớp nơi nó được xác định.



Hình 7 - Quan hệ giữa đảm bảo và gói đảm bảo tổng hợp

7 Các mức đảm bảo đánh giá

Các mức đảm bảo đánh giá (EAL) cung cấp một thang bậc tăng dần có cân bằng giữa mức độ đảm bảo đạt được với chi phí và tính khả thi đạt được cấp độ đảm bảo đó. TCVN 8709 xác định các khái

niệm khác nhau về đảm bảo trong TOE ở cuối của phần đánh giá, và duy trì sự đảm bảo đó trong quá trình sử dụng TOE.

Chú ý quan trọng rằng không phải tất cả các họ (families) và các thành phần (components) trong phần này của TCVN 8709 được bao gồm trong EAL. Điều này không phải nói rằng nó không cung cấp các đảm bảo có ý nghĩa và mong muốn. Thay vào đó nó được mong đợi rằng các họ và thành phần này sẽ xem xét thêm vào EAL trong các PP và ST

7.1 Tổng quan về các mức đảm bảo đánh giá (EAL)

Bảng 1 trình bầy một tổng kết của EAL. Các cột thể hiện một tập các EAL sắp xếp từ 1 đến 7, các dòng thể hiện các họ đảm bảo. Mỗi một số trong ma trận xác định một thành phần đảm bảo cụ thể có thể áp dụng được.

Như đã nêu ở phần sau, 7 cấp đảm bảo đánh giá được định nghĩa phân lớp trong TCVN 8709 nhằm đánh giá mức độ đảm bảo cho một TOE. Mức đảm bảo tăng lên từ EAL này đến EAL khác được thực hiện bởi việc thay thế một thành phần phần đảm bảo có cấp cao hơn từ cùng một họ đảm bảo (ví dụ tăng về tính chuẩn xác, phạm vi và/hoặc độ sâu) và từ việc thêm vào các thành phần đảm bảo từ các họ đảm bảo khác (ví dụ như thêm các yêu cầu mới).

Các EAL bao gồm một tổ hợp thích hợp các thành phần đảm bảo như được miêu tả trong phần 6 của TCVN 8709-3. Một cách chính xác hơn, mỗi EAL bao gồm không hơn một thành phần của mỗi họ bảo đảm và tất cả sự lệ thuộc đảm bảo của mỗi thành phần được xác định.

EAL được định nghĩa trong TCVN 8709, nó có thể được thể hiện bằng tổ hợp khác của sự đảm bảo. Đặc biệt, khái niệm "sự mở rộng" (augumentation) cho phép thêm vào các thành phần đảm bảo (từ họ đảm bảo không sẵn sàng trong EAL) hoặc thay thế thành phần đảm bảo (bằng một thành phần đảm bảo có cấp cao hơn trong cùng một họ đảm bảo) trong một EAL. Xây dựng nên sự đảm bảo được định nghĩa trong TCVN 8709, thì chỉ EAL có thể được mở rộng. Thuật ngữ "EAL trừ đi một thành phần đảm bảo" không được công nhận bởi chuẩn này. Khả năng mở rộng cho phép điều chỉnh tinh hữu ích và thêm giá trị vào thành phần đảm bảo mở rộng trong EAL. Một EAL có thể cũng được mở rộng với các yêu cầu đảm bảo rõ ràng.

Bảng 1 – Tóm tắt các cấp đảm bảo đánh giá

Lớp đảm bảo	Họ đảm bảo	Các thành phần đảm bảo theo các mức đảm bảo đánh giá (EAL)						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Phát triển	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Tài liệu hướng dẫn	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Hỗ trợ vòng đời	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Đánh giá đích an toàn	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1

	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Kiểm thử	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Đánh giá điểm yếu	AVA_VAN	1	2	2	3	4	5	5

7.2 Chi tiết cho mức đảm bảo đánh giá

Các phần sau trình bầy các định nghĩa của EAL, nêu rõ sự khác nhau giữa các yêu cầu cụ thể với các diễn tả văn xuôi của các yêu cầu đó sử dụng kiểu tô đậm.

7.3 Mức đảm bảo đánh giá mức 1 (EAL1) – Kiểm thử chức năng

7.3.1 Mục tiêu

EAL1 có thể áp dụng nơi mà tính bí mật trong hoạt động chính xác được yêu cầu, nhưng nguy cơ an toàn không được xem là quan trọng. Nó sẽ có giá trị khi sự bảo đảm độc lập được đòi hỏi để hỗ trợ luận điểm đã được áp dụng đối với sự bảo vệ thông tin cá nhân hoặc thông tin tương tự.

EAL1 chỉ đòi hỏi một đích an toàn giới hạn. Đơn giản chỉ là tuyên bố các yêu cầu chức năng an toàn (SFR) mà đích đánh giá (TOE) phải đáp ứng chứ không cần phải diễn giải xuất xứ của chúng xuất phát từ các nguy cơ đe dọa.

EAL1 đưa ra một đánh giá cho TOE đáp ứng cho khách hàng, bao gồm cả kiểm thử độc lập với một bảng mô tả đặc tính, và cung cấp một văn bản kiểm tra tài liệu hướng dẫn. Ý đồ hướng đến là đánh giá EAL1 có thể được thực hiện một cách thành công mà không cần sự trợ giúp của nhà phát triển TOE, và với chi phí nhỏ nhất.

Một đánh giá ở mức này có thể cung cấp bằng chứng về các chức năng TOE phù hợp với tài liệu của nó.

7.3.2 Các thành phần đảm bảo

EAL1 đưa ra một mức đảm bảo cơ bản bởi một đích an toàn giới hạn và sự phân tích các yêu cầu chức năng an toàn (SFR) trong đó ST sử dụng một đặc tả chức năng và giao diện kèm theo tài liệu hướng dẫn để diễn tả hoạt động an toàn.

Sự phân tích được hỗ trợ bởi việc tìm kiếm những điểm yếu tiềm năng thông báo công khai và kiểm tra độc lập các chức năng cũng như sự thâm nhập của các chức năng an toàn TOE (các TSF).

EAL1 cung cấp sự đảm bảo thông qua việc nhận dạng duy nhất cho TOE và tài liệu đánh giá liên quan.

EAL này có ý nghĩa hơn trong việc đảm bảo đối với một sản phẩm CNTT không được đánh giá.

Bảng 2 – EAL1

Lớp đảm bảo	Các thành phần đảm bảo
Phát triển: ADV	Đặc tả chức năng cơ bản (ADV_FSP.1)
Tài liệu hướng dẫn: AGD	Hướng dẫn người dùng vận hành (AGD_OPE.1)
	Các thủ tục chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời: ALC	Dán nhãn TOE (ALC_CMC.1)
	Tổng quát TOE CM (ALC_CMS.1)
Đánh giá đích an toàn: ASE	Yêu cầu tuân thủ (ASE_CCL.1)
	Định nghĩa các thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Các mục tiêu an toàn cho môi trường vận hành (ASE_OBJ.1)
	Các yêu cầu an toàn đã công bố (ASE_REQ.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Kiểm thử: ATE	Kiểm thử độc lập – Tuân thủ (ATE_IND.1)
Đánh giá điểm yếu: AVA	Khảo sát điểm yếu (AVA_VAN.1)

7.4 Mức đảm bảo đánh giá 2 (EAL2) – Kiểm thử cấu trúc

7.4.1 Mục tiêu

EAL2 yêu cầu sự hợp tác của nhà phát triển dưới dạng thông tin thiết kế và các kết quả kiểm tra, nhưng không yêu cầu nhiều hơn về tính hiệu quả của các bộ phận phát triển so với tính phù hợp thực tế về thương mại. Như vậy nó không yêu cầu một sự gia tăng về đầu tư chi phí và thời gian.

EAL2 vì vậy có thể áp dụng trong các trường hợp nhà phát triển và người sử dụng yêu cầu một mức thấp đến trung bình về đảm bảo an toàn một cách độc lập khi thiếu hồ sơ phát triển đầy đủ. Một tình huống như vậy có thể xảy ra khi đảm bảo cho các hệ thống kế thừa, hoặc ở nơi truy nhập đến nhà phát triển có thể bị giới hạn.

7.4.2 Các thành phần đảm bảo

EAL2 cung cấp sự đảm bảo bằng một đích an toàn đầy đủ và thông qua phân tích các đòi hỏi chức năng an toàn (SFR) của ST, sử dụng một đặc tả chức năng và giao diện, tài liệu hướng dẫn và các mô tả cơ sở về kiến trúc của TOE để hiểu hành vi an toàn.

Sự phân tích được hỗ trợ bằng việc kiểm tra độc lập các chức năng an toàn TOE, bằng chứng về việc kiểm tra của nhà phát triển dựa trên đặc tính chức năng, sự xác nhận độc lập có chọn lọc các kết quả kiểm tra của nhà phát triển, phân tích những điểm yếu (dựa trên các đặc tính chức năng, thiết kế TOE, mô tả kiến trúc an toàn và bằng chứng hướng dẫn được cung cấp) để thể hiện khả năng phản ứng trước một xâm nhập của kẻ tấn công với một tiền lực tấn công cơ sở.

EAL2 cũng cung cấp sự đảm bảo thông qua hệ thống quản lý cấu hình và bằng chứng của các thủ tục chuyển giao an toàn.

EAL này thể hiện sự đảm bảo có ý nghĩa hơn so với EAL1 bằng việc yêu cầu kiểm tra của nhà phát triển, phân tích lỗ hổng, (ngoài ra tìm kiếm thông tin công cộng) và kiểm tra độc lập dựa trên đặc tả TOE chi tiết hơn.

Bảng 3 – EAL 2

Lớp đảm bảo	Các thành phần đảm bảo
Phát triển: ADV	Đặc tả kiến trúc an toàn (ADV_ARC.1)
	Đặc tả chức năng bắt buộc an toàn (ADV_FSP.2)
	Thiết kế cơ bản (ADV_TDS.1)
Tài liệu hướng dẫn: AGD	Hướng dẫn người dùng vận hành (AGD_OPE.1)
	Các thủ tục chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời: ALC	Sử dụng một hệ thống CM (ALC_CMC.2)
	Các phần tổng quát TOE CM (ALC_CMS.2)
	Các thủ tục chuyển giao (ALC_DEL.1)
Đánh giá đích an toàn: ASE	Yêu cầu tuân thủ (ASE_CCL.1)
	Định nghĩa các thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Các mục tiêu an toàn (ASE_OBJ.2)
	Các yêu cầu an toàn thu được (ASE_REQ.2)
	Định nghĩa vấn đề an toàn (ASE_SPD.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Kiểm thử: ATE	Chứng cứ về tính tổng quát (ATE_COV.1)
	Kiểm thử chức năng (ATE_FUN.1)
	Kiểm thử độc lập – ví dụ (ATE_IND.2)
Đánh giá điểm yếu: AVA	Phân tích điểm yếu (AVA_VAN.2)

7.5 Mức đảm bảo đánh giá 3 (EAL3) – Kiểm thử và kiểm tra phương pháp

7.5.1 Mục tiêu

EAL3 cho phép một nhà phát triển tận tâm đạt được sự đảm bảo tối đa với công nghệ an toàn tốt ở mức thiết kế mà không cần thay đổi các cơ chế phát triển đang có sẵn.

EAL3 có thể ứng dụng trong các tình huống mà nhà phát triển hoặc người sử dụng yêu cầu ở mức vừa phải về đảm bảo an toàn độc lập, và yêu cầu một sự điều tra tỉ mỉ về TOE và phát triển nó không cần bước thiết kế lại đáng kể nào.

7.5.2 Các thành phần đảm bảo

EAL3 cung cấp đảm bảo bởi một đích an toàn đầy đủ và phân tích các yêu cầu chức năng an toàn (SFR) của ST, sử dụng một đặc tả chức năng và giao diện, tài liệu hướng dẫn và các mô tả về kiến trúc thiết kế của TOE, để diễn giải hoạt động an toàn.

Sự phân tích được hỗ trợ bằng việc kiểm tra một cách độc lập các chức năng an toàn của TOE, chứng cứ về việc kiểm thử của nhà phát triển dựa trên đặc tả chức năng và thiết kế TOE, sự xác nhận độc lập có chọn lọc các kết quả kiểm tra của nhà phát triển, phân tích các lỗ hổng/điểm yếu (dựa trên các đặc tính chức năng, thiết kế TOE, mô tả kiến trúc an toàn và bằng chứng hướng dẫn được cung cấp) để thể hiện khả năng bảo vệ trước xâm nhập của kẻ tấn công với một tiềm lực tấn công cơ bản.

EAL3 cung cấp đảm bảo thông qua sử dụng các biện pháp quản lý môi trường phát triển, quản lý cấu hình TOE, và chứng cứ về các thủ tục chuyển giao an toàn.

EAL này thể hiện sự đảm bảo có ý nghĩa hơn so với EAL2 bằng việc đòi hỏi tổng quát việc kiểm thử hoàn thiện hơn về chức năng an toàn và cơ chế và/hoặc thủ tục nhằm đưa ra một sự tin cậy nào đó về việc TOE sẽ không bị giả mạo trong quá trình phát triển.

Bảng 4 – EAL3

Lớp đảm bảo	Các thành phần đảm bảo
Phát triển: ADV	Đặc tả kiến trúc an toàn (ADV_ARC.1)
	Đặc tả chức năng với tóm tắt đầy đủ (ADV_FSP.3)
	Thiết kế kiến trúc (ADV_TDS.2)
Tài liệu hướng dẫn: AGD	Hướng dẫn người dùng vận hành (AGD_OPE.1)
	Các thủ tục chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời: ALC	Các biện pháp quản lý cấp quyền (ALC_CMC.3)
	Tổng quát CM biểu diễn triển khai (ALC_CMS.3)
	Các thủ tục chuyển giao (ALC_DEL.1)
	Định danh các biện pháp an toàn (ALC_DVS.1)
	Mô hình vòng đời định nghĩa cho nhà phát triển (ALC_LCD.1)
Đánh giá đích an toàn: ASE	Yêu cầu tuân thủ (ASE_CCL.1)
	Định nghĩa các thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Các mục tiêu an toàn (ASE_OBJ.2)
	Các yêu cầu an toàn thu được (ASE_REQ.2)
	Định nghĩa vấn đề an toàn (ASE_SPD.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Kiểm thử: ATE	Phân tích tổng quát (ATE_COV.2)
	Kiểm thử: Thiết kế cơ bản (ATE_DPT.1)
	Kiểm thử chức năng (ATE_FUN.1)
	Kiểm thử độc lập – ví dụ (ATE_IND.2)
Đánh giá điểm yếu: AVA	Phân tích điểm yếu (AVA_VAN.2)

7.6 Mức đảm bảo đánh giá 4 (EAL4) – Thiết kế, kiểm thử, soát xét phương pháp

7.6.1 Mục tiêu

EAL4 cho phép một nhà phát triển đạt được sự đảm bảo tối đa về kỹ thuật an toàn tốt dựa trên các thực tế phát triển thương mại tốt, tuy chặt chẽ, song không yêu cầu kiến thức chuyên gia, kỹ năng, và các tài nguyên đáng kể nào khác. EAL4 là mức cao nhất khả thi về mặt kinh tế đưa vào một dòng sản phẩm đang tồn tại.

EAL4 vì vậy có thể ứng dụng trong các trường hợp mà ở đó các nhà phát triển và người sử dụng yêu cầu một mức từ trung bình đến cao đảm bảo an toàn độc lập trong TOE thông thường và được chuẩn bị để đưa vào các chi phí mở rộng công trình an toàn cụ thể.

7.6.2 Các thành phần đảm bảo

EAL4 cung cấp khả năng đảm bảo bởi một đích an toàn đầy đủ và sự phân tích các yêu cầu chức năng an toàn (SFR) của ST, sử dụng một đặc tả chức năng và giao diện, tài liệu hướng dẫn, mô tả về thiết kế mô-đun cơ bản của TOE và một tập triển khai, nhằm diễn giải hoạt động an toàn.

Sự phân tích được hỗ trợ bởi việc kiểm tra độc lập các chức năng an toàn TOE, chứng cứ về việc kiểm thử của nhà phát triển dựa trên đặc tả chức năng và thiết kế của TOE, sự khẳng định độc lập có lựa chọn về các kết quả kiểm thử của nhà phát triển, phân tích các lỗ hổng/điểm yếu (dựa trên các đặc tính chức năng, thiết kế TOE, trình diễn thực thi, thiết kế kiến trúc và bằng chứng hướng dẫn được cung cấp) để thể hiện khả năng bảo vệ trước xâm nhập của kẻ tấn công với một tiềm lực tấn công trên mức cơ bản.

EAL4 cũng cung cấp đảm bảo thông qua sử dụng các biện pháp quản lý môi trường phát triển và quản lý cấu hình TOE mở rộng bao gồm tự động hóa và bằng chứng về các thủ tục chuyển giao an toàn

EAL này thể hiện sự đảm bảo hơn EAL3 bằng việc yêu cầu mô tả thiết kế tỉ mỉ hơn, trình diễn thực thi cho toàn bộ các chức năng an toàn TOE và cơ chế cải thiện và/hoặc các thủ tục nhằm đưa ra sự tin cậy rằng TOE sẽ không bị giả mạo trong quá trình phát triển.

Bảng 5 – EAL4

Lớp đảm bảo	Các thành phần đảm bảo
Phát triển: ADV	Đặc tả kiến trúc an toàn (ADV_ARC.1)
	Đặc tả chức năng đầy đủ (ADV_FSP.4)
	Mô tả triển khai TSF (ADV_IMP.1)
	Thiết kế kiến trúc cơ sở (ADV_TDS.3)
Tài liệu hướng dẫn: AGD	Hướng dẫn người dùng vận hành (AGD_OPE.1)
	Các thủ tục chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời: ALC	Tự động hóa, các thủ tục chấp nhận và hỗ trợ sản xuất (ALC_CMC.4)
	Tổng quát CM theo dấu vết vấn đề (ALC_CMS.4)
	Các thủ tục chuyển giao (ALC_DEL.1)
	Định danh các biện pháp an toàn (ALC_DVS.1)
	Mô hình vòng đời định nghĩa cho nhà phát triển (ALC_LCD.1)
	Các công cụ phát triển xác định rõ (ALC_TAT.1)
Đánh giá đích an toàn: ASE	Yêu cầu tuân thủ (ASE_CCL.1)
	Định nghĩa các thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Các mục tiêu an toàn (ASE_OBJ.2)
	Các yêu cầu an toàn thu được (ASE_REQ.2)
	Định nghĩa vấn đề an toàn (ASE_SPD.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Kiểm thử: ATE	Phân tích tổng quát (ATE_COV.2)
	Kiểm thử: Các mô đun bắt buộc an toàn (ATE_DPT.2)
	Kiểm thử chức năng (ATE_FUN.1)
	Kiểm thử độc lập – ví dụ (ATE_IND.2)
Đánh giá điểm yếu: AVA	Phân tích điểm yếu trọng tâm (AVA_VAN.3)

7.7 Mức đảm bảo đánh giá 5 (EAL5) – Thiết kế và kiểm thử bán chính thức

7.7.1 Mục tiêu

EAL5 cho phép một nhà phát triển đạt được đảm bảo tối đa với kỹ thuật an toàn dựa trên thực tế sự phát triển thương mại nghiêm ngặt hỗ trợ bởi việc ứng dụng ở mức trung bình các kỹ thuật an toàn đặc biệt. Như vậy một TOE sẽ có thể được thiết kế và phát triển với mục đích đạt được đảm bảo EAL5. Nó tương tự như các chi phí mở rộng đưa vào các yêu cầu EAL5, liên quan đến sự phát triển nghiêm ngặt không ứng dụng các kỹ thuật đặc biệt.

EAL5 vì vậy có khả năng ứng dụng trong các trường hợp mà ở đó nhà phát triển và người sử dụng yêu cầu ở mức cao đảm bảo an toàn độc lập trong sự phát triển đã được kế hoạch và đòi hỏi một nghiên cứu phát triển nghiêm ngặt không chịu các chi phí có thể quy cho các kỹ thuật an toàn đặc biệt.

7.7.2 Các thành phần đảm bảo.

EAL5 cung cấp khả năng đảm bảo bằng một đích an toàn đầy đủ và việc phân tích các đòi hỏi chức năng an toàn (SFR) của ST, sử dụng một đặc tả chức năng và giao diện, tài liệu hướng dẫn, mô tả thiết kế của TOE, và ứng dụng, để hiểu hành vi an toàn. Như vậy đòi hỏi TSF thiết kế theo mô-đun.

Sự phân tích được hỗ trợ bởi việc kiểm tra độc lập các chức năng an toàn TOE, bằng chứng kiểm tra nhà phát triển dựa trên các đặc tả chức năng, thiết kế TOE, sự khẳng định độc lập có lựa chọn các kết quả kiểm tra nhà phát triển, và một sự phân tích lỗ hổng độc lập thể hiện sự phản ứng đối với các xâm nhập của kẻ tấn công với một khả năng tấn công mức vừa phải.

EAL5 cũng cung cấp khả năng đảm bảo thông qua sử dụng các kiểm soát môi trường phát triển, và quản lý cấu hình TOE tổng thể bao gồm thông tin và bằng chứng của các thủ tục chuyển giao an toàn.

EAL này thể hiện sự đảm bảo hơn EAL4 bằng việc yêu cầu mô tả thiết kế bán chính thức, kiến trúc có cấu trúc hơn (và từ đây có thể phân tích) và cơ chế cải thiện và/hoặc các thủ tục mà nó cung cấp sự chắc chắn mà TOE sẽ không bị ảnh hưởng trong quá trình phát triển.

Bảng 6 – EAL5

Lớp đảm bảo	Các thành phần đảm bảo
Phát triển: ADV	Đặc tả kiến trúc an toàn (ADV_ARC.1)
	Đặc tả chức năng đầy đủ bán chính thức với thông tin lỗi bổ sung (ADV_FSP.5)
	Mô tả triển khai TSF (ADV_IMP.1)
	Thiết kế mô đun bán chính thức (ADV_TDS.4)
Tài liệu hướng dẫn: AGD	Hướng dẫn người dùng vận hành (AGD_OPE.1)
	Các thủ tục chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời: ALC	Tự động hóa, các thủ tục chấp nhận và hỗ trợ sản xuất (ALC_CMC.4)
	Tổng quát CM các công cụ phát triển (ALC_CMS.5)
	Các thủ tục chuyển giao (ALC_DEL.1)
	Định danh các biện pháp an toàn (ALC_DVS.1)
	Mô hình vòng đời định nghĩa cho nhà phát triển (ALC_LCD.1)
	Tuân thủ với các tiêu chuẩn triển khai (ALC_TAT.2)
Đánh giá đích an toàn: ASE	Yêu cầu tuân thủ (ASE_CCL.1)
	Định nghĩa các thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Các mục tiêu an toàn (ASE_OBJ.2)

	Các yêu cầu an toàn thu được (ASE_REQ.2)
	Định nghĩa vấn đề an toàn (ASE_SPD.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Kiểm thử: ATE	Phân tích tổng quát (ATE_COV.2)
	Kiểm thử: Thiết kế mô đun (ATE_DPT.3)
	Kiểm thử chức năng (ATE_FUN.1)
	Kiểm thử độc lập – ví dụ (ATE_IND.2)
Đánh giá điểm yếu: AVA	Phân tích điểm yếu theo phương pháp (AVA_VAN.4)

7.8 Mức đảm bảo đánh giá 6 (EAL6) – Xác minh thiết kế và kiểm thử bán chính thức

7.8.1 Mục tiêu

EAL6 cho phép nhà phát triển đạt tới độ đảm bảo cao từ việc ứng dụng các kỹ thuật an toàn đối với môi trường phát triển nghiêm ngặt để đưa ra TOE cho việc bảo vệ bảo vệ dữ liệu có giá trị cao trước các rủi ro.

EAL6 vì vậy có thể ứng dụng để phát triển TOE cho ứng dụng có độ rủi ro cao mà ở đó giá trị của tài sản bảo vệ điều chỉnh theo chi phí phát sinh.

7.8.2 Các thành phần đảm bảo

EAL6 cung cấp khả năng đảm bảo bởi một đích an toàn đầy đủ và sự phân tích các yêu cầu chức năng an toàn (SFR) của ST, sử dụng đặc tả chức năng và giao diện tổng thể, tài liệu hướng dẫn, thiết kế của TOE, và triển khai, nhằm diễn giải hoạt động an toàn. Ngoài ra, đảm bảo còn đạt được thông qua một mô hình chính thức về lựa chọn các chính sách an toàn TOE và một thể hiện bán chính thức của các đặc tả chức năng, thiết kế TOE. Điều đó đòi hỏi thiết kế TOE theo mô-đun và phân lớp.

Sự phân tích được hỗ trợ bởi việc kiểm tra độc lập các chức năng an toàn TOE, bằng chứng về việc kiểm thử của nhà phát triển dựa trên đặc tả chức năng, thiết kế TOE, sự xác nhận độc lập có lựa chọn về các kết quả kiểm thử của nhà phát triển, và một sự phân tích lỗ hổng độc lập thể hiện bảo vệ trước xâm nhập của kẻ tấn công với một khả năng tấn công mức cao.

EAL6 cũng cung cấp khả năng đảm bảo thông qua sử dụng một quy trình phát triển có cấu trúc, các biện pháp quản lý môi trường phát triển, và quản lý cấu hình TOE tổng thể bao gồm thông tin và bằng chứng của các thủ tục chuyển giao an toàn.

EAL này đưa ra một sự đảm bảo có ý nghĩa hơn so với EAL5 bằng việc yêu cầu sự phân tích toàn diện hơn, thể hiện ứng dụng có cấu trúc, kiến trúc có cấu trúc hơn (ví dụ phân lớp), sự phân tích lỗ hổng độc lập toàn diện hơn, cải thiện quản lý cấu hình và kiểm soát môi trường phát triển.

Bảng 7 – EAL6

Lớp đảm bảo	Các thành phần đảm bảo
Phát triển: ADV	Đặc tả kiến trúc an toàn (ADV_ARC.1)
	Đặc tả chức năng đầy đủ bán chính thức với thông tin lỗi bổ sung (ADV_FSP.5)
	Ánh xạ đầy đủ mô tả triển khai TSF (ADV_IMP.2)
	Nội bộ tổ hợp tối thiểu (ADV_INT.3)
	Mô hình chính sách an toàn TOE chính thức (ADV_SPM.1)
	Thiết kế mô đun đầy đủ bán chính thức (ADV_TDS.5)

Tài liệu hướng dẫn: AGD	Hướng dẫn người dùng vận hành (AGD_OPE.1)
	Các thủ tục chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời: ALC	Hỗ trợ cải tiến (ALC_CMC.5)
	Tổng quát CM các công cụ phát triển (ALC_CMS.5)
	Các thủ tục chuyển giao (ALC_DEL.1)
	Sự đầy đủ của các biện pháp an toàn (ALC_DVS.2)
	Mô hình vòng đời định nghĩa cho nhà phát triển (ALC_LCD.1)
	Tuân thủ với các tiêu chuẩn triển khai – tất cả các phần (ALC_TAT.3)
Đánh giá đích an toàn: ASE	Yêu cầu tuân thủ (ASE_CCL.1)
	Định nghĩa các thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Các mục tiêu an toàn (ASE_OBJ.2)
	Các yêu cầu an toàn thu được (ASE_REQ.2)
	Định nghĩa vấn đề an toàn (ASE_SPD.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Kiểm thử: ATE	Phân tích tổng quát nghiêm ngặt (ATE_COV.3)
	Kiểm thử: Thiết kế mô đun (ATE_DPT.3)
	Kiểm thử chức năng theo thứ tự (ATE_FUN.2)
	Kiểm thử độc lập – ví dụ (ATE_IND.2)
Đánh giá điểm yếu: AVA	Phân tích điểm yếu theo phương pháp cải tiến (AVA_VAN.5)

7.9 Mức đảm bảo đánh giá 7 (EAL7) –Xác minh thiết kế và kiểm thử chính thức

7.9.1 Mục tiêu

EAL7 được ứng dụng để phát triển TOE cho ứng dụng có độ rủi ro rất cao và hoặc ở đó tài sản có giá trị cao điều chỉnh chi phí lớn hơn. Ứng dụng thực tế của EAL7 hiện nay giới hạn cho TOE tập trung vào chức năng an toàn tuân theo phân tích chính thức mở rộng.

7.9.2 Các thành phần đảm bảo

EAL7 cung cấp khả năng đảm bảo bởi một đích an toàn đầy đủ và sự phân tích các yêu cầu chức năng an toàn (SFRs) của ST, sử dụng đặc tả chức năng và giao diện tổng thể, tài liệu hướng dẫn, thiết kế TOE, và một thể hiện triển khai có cấu trúc, nhằm diễn giải hoạt động an toàn. Ngoài ra, đảm bảo còn đạt được thông qua một mô hình chính thức về chọn lựa các chính sách an toàn TOE, và một thể hiện bán chính thức các đặc tả chức năng và thiết kế TOE. Điều đó đòi hỏi thiết kế TSF có tính mô-đun, đơn giản và có phân lớp.

Sự phân tích được hỗ trợ bởi việc kiểm thử độc lập các chức năng an toàn TOE, bằng chứng về việc kiểm thử của nhà phát triển dựa trên đặc tả chức năng, thiết kế TOE và thể hiện triển khai, xác nhận độc lập có lựa chọn về các kết quả kiểm tra của nhà phát triển, một phân tích lỗ hổng độc lập thể hiện sự bảo vệ trước xâm nhập của kẻ tấn công với một khả năng tấn công mức cao.

EAL7 cũng cung cấp khả năng đảm bảo thông qua sử dụng một quy trình phát triển có cấu trúc, các biện pháp quản lý môi trường phát triển, quản lý cấu hình TOE tổng thể bao gồm tự động hóa đầy đủ và bằng chứng về các thủ tục chuyển giao an toàn.

EAL này đưa ra một sự đảm bảo có ý nghĩa hơn so với EAL6 bằng việc yêu cầu phân tích toàn diện hơn, sử dụng các thể diện chính thức, phù hợp chính thức và kiểm thử toàn diện.

Bảng 8 – EAL7

Lớp đảm bảo	Các thành phần đảm bảo
Phát triển: ADV	Đặc tả kiến trúc an toàn (ADV_ARC.1)
	Đặc tả chức năng đầy đủ bán chính thức với đặc tả chính thức bổ sung (ADV_FSP.6)
	Ánh xạ đầy đủ mô tả triển khai TSF (ADV_IMP.2)
	Nội bộ tổ hợp tối thiểu (ADV_INT.3)
	Mô hình chính sách an toàn TOE chính thức (ADV_SPM.1)
	Thiết kế mô đun đầy đủ bán chính thức với thể hiện thiết kế mức cao (ADV_TDS.6)
Tài liệu hướng dẫn: AGD	Hướng dẫn người dùng vận hành (AGD_OPE.1)
	Các thủ tục chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời: ALC	Hỗ trợ cải tiến (ALC_CMC.5)
	Tổng quát CM các công cụ phát triển (ALC_CMS.5)
	Các thủ tục chuyển giao (ALC_DEL.1)
	Sự đầy đủ của các biện pháp an toàn (ALC_DVS.2)
	Mô hình vòng đời định mức được (ALC_LCD.2)
	Tuân thủ với các tiêu chuẩn triển khai – tất cả các phần (ALC_TAT.3)
Đánh giá đích an toàn: ASE	Yêu cầu tuân thủ (ASE_CCL.1)
	Định nghĩa các thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Các mục tiêu an toàn (ASE_OBJ.2)
	Các yêu cầu an toàn thu được (ASE_REQ.2)
	Định nghĩa vấn đề an toàn (ASE_SPD.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Kiểm thử: ATE	Phân tích tổng quát nghiêm ngặt (ATE_COV.3)
	Kiểm thử: Biểu diễn triển khai (ATE_DPT.4)
	Kiểm thử chức năng theo thứ tự (ATE_FUN.2)
	Kiểm thử độc lập – đầy đủ (ATE_IND.3)
Đánh giá điểm yếu: AVA	Phân tích điểm yếu theo phương pháp cải tiến (AVA_VAN.5)

8 Các gói đảm bảo tổng hợp

Các gói đảm bảo tổng hợp (CAP) cung cấp một thang đo tăng dần để cân bằng mức độ đảm bảo đạt được với giá thành và sự khả thi có thể đạt được mà mức độ đảm bảo cho TOE tổng hợp.

Điểm quan trọng cần chú ý là chỉ có một số lượng nhỏ các họ và thành phần trong phần này của ISO 15408 được chứa trong CAP. Đây là tính tất yếu của việc xây dựng dựa trên các kết quả đánh giá các thực thể được đánh giá trước đó (dựa trên các thành phần và các thành phần phụ thuộc), điều này không nói lên rằng chúng không cung cấp các đảm bảo được mong muốn và đầy đủ ý nghĩa.

8.1 Tổng quan về gói đảm bảo tổng hợp (CAP)

CAP có thể được sử dụng để đưa ra các TOE tổng hợp, bao gồm các thành phần mà đã hoặc sẽ được đánh giá TOE thành phần (xem Phụ lục B). Các thành phần riêng sẽ được chứng nhận EAL hoặc gói bảo đảm khác được chỉ ra trong ST. Với mong muốn, mức độ cơ bản của bảo đảm trong TOE thành phần sẽ đạt được thông qua áp dụng các EAL1, mà có thể đạt được với các thông tin về thành phần

thường có sẵn trong một miền chung. (EAL1 có thể được áp dụng như được chỉ ra trong cả TOE tổng hợp và thành phần). CAP cung cấp một cách tiếp cận khác để đạt được cấp độ cao hơn bảo đảm cho TOE thành phần hơn việc áp dụng các EAL trên EAL1.

Khi một thành phần phụ thuộc có thể được đánh giá bằng cách sử dụng các đánh giá và chứng nhận trước đó để thỏa mãn đòi hỏi về nền tảng CNTT trong môi trường, điều này không cung cấp bất kỳ sự bảo đảm chính thức của tương tác giữa các thành phần hoặc đưa ra các lỗ hổng có thể xảy ra thu được từ sự tổng hợp. Các gói đảm bảo tổng hợp xem xét các tương tác này, ở các mức đảm bảo cao hơn, đảm bảo rằng tương tác giữa các thành phần mà chính nó là mục tiêu để kiểm thử. Phân tích điểm yếu của TOE tổng hợp sẽ được thực hiện để xem xét việc đưa ra các điểm yếu như là kết quả của sự tổng hợp các thành phần.

Bảng 9 biểu diễn tóm tắt của các CAP. Các cột biểu diễn sự phân cấp có trật tự của các tập của các CAP, còn các hàng biểu diễn các họ đảm bảo. Mỗi số trong ma trận kết quả chỉ ra một thành phần đảm bảo tại các chỗ có thể áp dụng.

Như được nêu trong mục con tiếp theo, ba gói đảm bảo tổng hợp được phân cấp có trật tự được định nghĩa trong TCVN 8709 để xếp hạng mức độ đảm bảo của các TOE tổng hợp. Chúng được phân cấp theo trật tự để đảm bảo rằng mỗi biểu diễn CAP là chính xác hơn tất cả CAP thấp hơn. Việc tăng mức độ đảm bảo từ CAP đến CAP được thực hiện bằng việc thay thế bằng thành phần đảm bảo có mức độ phân cấp cao hơn từ các họ đảm bảo tương tự (ví dụ tăng tính nghiêm ngặt, phạm vi và độ sâu) và từ việc bổ xung các thành phần đảm bảo từ các họ đảm bảo khác (ví dụ như thêm các đòi hỏi mới). Điều này làm việc phân tích lớn hơn với các tập hợp để chỉ ra tác động trong các kết quả đánh giá đạt được với TOE tổng hợp.

Các CAP bao gồm một sự phối hợp thích hợp của các thành phần đảm bảo như mô tả trong điều 6 trong phần TCVN 8709 này. Chính xác hơn, mỗi CAP chứa không nhiều hơn một thành phần của mỗi họ đảm bảo và tất cả các phụ thuộc đảm bảo trong mọi thành phần được đề cập đến.

Các CAP chỉ xem xét khả năng chống lại kẻ tấn công với khả năng tấn công lên trên mức cơ bản. Đây là do mức độ thông tin thiết kế được cung cấp bởi ACO_DEV, hạn chế một số yếu tố kết hợp với khả năng tấn công (hiểu biết về các thành phần cấu thành TOE) và sau đó ảnh hưởng đến sự chặt chẽ của phân tích yếu điểm được thực hiện bởi đánh giá viên. Vì vậy, mức độ đảm bảo trong TOE tổng hợp sẽ bị giới hạn, mặc dù vậy việc đảm bảo trong các thành phần riêng trong TOE tổng hợp cao hơn nhiều.

Bảng 9 – Tóm tắt mức đảm bảo tổng hợp

Lớp đảm bảo	**Họ đảm bảo**	**Các thành phần đảm bảo từ Gói đảm bảo tổng hợp**		
		CAP-A	CAP-B	CAP-C
Tổng hợp	ACO_COR	**1**	**1**	1
	ACO_CTT	**1**	**2**	2
	ACO_DEV	**1**	**2**	**3**
	ACO_REL	**1**	1	**2**
	ACO_VUL	**1**	**2**	**3**
Tài liệu hướng dẫn	AGD_OPE	**1**	1	1
	AGD_PRE	**1**	1	1
Hỗ trợ vòng đời	ACL_CMC	**1**	1	1
	ACL_CMS	**2**	2	2
	ACL_DEL			
	ACL_DVS			
	ACL_FLR			

	ACL_LCD			
	ACL_TAT			
Đánh giá đích an toàn	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD		1	1
	ASE_TSS	1	1	1

8.2 Chi tiết về gói đảm bảo tổng hợp

Các điều khoản sau đây sẽ cung cấp các định nghĩa của các CAP, phần khác nhau giữa các yêu cầu riêng và các đặc trưng thường của các yêu cầu này sử dụng chữ in đậm.

8.3 Mức đảm bảo tổng hợp A (CAP-A) – Tổng hợp theo cấu trúc

8.3.1 Mục tiêu

CAP-A được áp dụng khi TOE tổng hợp được tích hợp và tin cậy với hoạt động an toàn thực hiện đúng theo tổng hợp kết quả được yêu cầu. Điều này đòi hỏi sự hợp tác của nhà phát triển của thành phần phụ thuộc về việc cung cấp thông tin thiết kế và kết quả kiểm tra từ việc chứng nhận các thành phần phụ thuộc, mà không đòi hỏi sự tham gia của nhà phát triển thành phần cơ sở.

CAP-A do đó áp dụng trong các trường hợp này, nơi các nhà phát triển hoặc người dùng yêu cầu một mức thấp đến trung bình mức độ an toàn được đảm bảo một cách độc lập trong trường hợp không sẵn có toàn bộ bản ghi phát triển.

8.3.2 Các thành phần đảm bảo

CAP-A cung cấp đảm bảo thông qua phân tích đích an toàn cho TOE tổng hợp. Các SFR trong ST của TOE tổng hợp được phân tích bằng cách sử dụng kết quả đầu ra từ đánh giá của các TOE thành phần (ví dụ ST, tài liệu hướng dẫn) và đặc tả cho các giao diện giữa các TOE thành phần trong TOE tổng hợp để hiểu về hành vi an toàn.

Phân tích này được hỗ trợ bằng cách kiểm tra độc lập của các giao diện của các thành phần cơ sở dựa trên thành phần phụ thuộc, như được mô tả trong thông tin tin cậy, bằng chứng về nhà phát triển các phép thử dựa trên thông tin tin cậy, thông tin phát triển và các sở cứ tổng hợp, và lựa chọn xác nhận độc lập có chọn lọc các kết quả kiểm tra của nhà phát triển. Phân tích này cũng được hỗ trợ bởi việc xem xét lại điểm yếu trong TOE tổng hợp bởi đánh giá viên.

CAP-A cũng cung cấp bảo đảm thông qua nhận dạng duy nhất của TOE tổng hợp (ví dụ TOE CNTT và tài liệu hướng dẫn).

Bảng 10 – CAP-A

Lớp đảm bảo	Các thành phần đảm bảo
ACO: Tổng hợp	ACO_COR.1 Sở cứ tổng hợp
	ACO_CTT.1 Kiểm thử giao diện
	ACO_DEV.1: Mô tả chức năng
	ACO_REL.1: Thông tin tin cậy cơ sở
	ACO_VUL.1: Soát xét các điểm yếu tổng hợp

AGD: Tài liệu hướng dẫn	AGD_OPE.1 Hướng dẫn người dùng vận hành
	AGD_PRE.1 Các thủ tục chuẩn bị
ALC: Hỗ trợ vòng đời	ACL_CMC.1 Gắn nhãn cho TOE
	ACL_CMS.2: Các phần của TOE CM tổng quát
Đánh giá các đích an toàn	ASE_CCL.1 Các yêu cầu tuân thủ
	ASE_ECD.1 Định nghĩa các thành phần mở rộng
	ASE_INT.1: Giới thiệu ST
	ASE_OBJ.1: Các mục tiêu an toàn cho môi trường vận hành
	ASE_REQ.1: Các yêu cầu an toàn đã xác nhận
	ASE_TSS.1: Đặc tả tổng quát TOE

8.4 Mức đảm bảo tổng hợp B (CAP-B) – Tổng hợp theo phương pháp

8.4.1 Mục tiêu

CAP-B cho phép nhà phát triển đạt được đảm bảo tối đa từ sự hiểu biết, tại mức hệ thống con, các ảnh hưởng của tương tác giữa các TOE thành phần được tích hợp trong các TOE tổng hợp, trong khi giảm thiểu nhu cầu về sự tham gia của các nhà phát triển thành phần cơ sở.

CAP-B được áp dụng trong các trường hợp này, nơi các nhà phát triển hay người dùng đòi hỏi một mức độ vừa phải về an toàn được đảm bảo độc lập, và yêu cầu một cuộc điều tra kỹ lưỡng về TOE tổng hợp và sự phát triển của nó mà không có kỹ thuật quan trọng.

8.4.2 Các thành phần đảm bảo

CAP-B cung cấp đảm bảo bằng phân tích một đích an toàn đầy đủ cho TOE tổng hợp. Các SFR trong ST của TOE tổng hợp sẽ được phân tích bằng cách sử dụng kết quả đầu ra từ đánh giá của các TOE thành phần (ví dụ như ST, tài liệu hướng dẫn), đặc tả cho các giao diện giữa các TOE thành phần **và thiết kế TOE (mô tả hệ thống con TSF) chứa** trong thông tin phát triển tổng hợp để hiểu về các hành vi an toàn.

Phân tích này được hỗ trợ bằng cách kiểm tra độc lập của các giao diện của thành phần cơ sở được dựa trên các thành phần phụ thuộc, như mô tả trong thông tin tin cậy **(bây giờ cũng bao gồm thiết kế TOE)**, bằng chứng kiểm thử phát triển dựa trên thông tin tin cậy, thông tin phát triển và sở cứ tạo ra, xác nhận độc lập có chọn lọc kết quả kiểm thử của nhà phát triển. Phân tích cũng được hỗ trợ bởi một phân tích điểm yếu trong TOE tổng hợp bởi đánh giá viên chứng minh khả năng chống kẻ tấn công với các khả năng tấn công.

CAP biểu diễn sự gia tăng có ý nghĩa trong sự bảo đảm từ CAP-A bằng cách yêu cầu vùng bao phủ đầy đủ hơn của các chức năng an toàn.

Bảng 11 – CAP-B

Lớp đảm bảo	Các thành phần đảm bảo
ACO: Tổng hợp	ACO_COR.1 Sở cứ tổng hợp
	ACO_CTT.2 Kiểm thử giao diện nghiêm ngặt
	ACO_DEV.2: Mô tả chứng cứ cơ sở
	ACO_REL.1: Thông tin tin cậy cơ sở
	ACO_VUL.2: Soát xét các điểm yếu thành phần
AGD: Tài liệu hướng	AGD_OPE.1 Hướng dẫn người dùng vận hành

dẫn	AGD_PRE.1 Các thủ tục chuẩn bị
ALC: Hỗ trợ vòng đời	ACL_CMC.1 Gắn nhãn cho TOE
	ACL_CMS.2: Các phần của TOE CM tổng quát
Đánh giá các đích an toàn	ASE_CCL.1 Các yêu cầu tuân thủ
	ASE_ECD.1 Định nghĩa các thành phần mở rộng
	ASE_INT.1: Giới thiệu ST
	ASE_OBJ.2: Các mục tiêu an toàn
	ASE_REQ.2: Các yêu cầu an toàn được cung cấp
	ASE_SPD.1 Định nghĩa các vấn đề an toàn
	ASE_TSS.1: Đặc tả tổng quát TOE

8.5 Mức đảm bảo tổng hợp C (CAP-C) – Tổng hợp theo phương pháp, kiểm tra và soát xét.

8.5.1 Mục tiêu

CAP-C cho phép nhà phát triển đạt được mức đảm bảo cao nhất từ việc phân tích chủ động sự tương tác giữa các thành phần của TOE tổng hợp, mà không đòi hỏi phải truy cập đầy đủ đến tất cả các chứng cứ đánh giá của thành phần cơ sở.

CAP-C do đó áp dụng trong các trường hợp này, nơi các nhà phát triển hoặc người sử dụng đòi hỏi phải có mức độ an toàn độc lập được đảm bảo ở mức trung bình đến cao trong TOE tổng hợp thông thường truyền thống và được chuẩn bị để phải chịu thêm chi phí liên quan đến vấn đề an toàn đặc trưng.

8.5.2 Các thành phần đảm bảo

CAP-C cung cấp đảm bảo bằng phân tích của một đích an toàn đầy đủ cho TOE tổng hợp. Các SFR trong ST của TOE tổng hợp được phân tích bằng cách sử dụng kết quả đầu ra thông qua đánh giá các TOE thành phần (ví dụ như ST, tài liệu hướng dẫn), đặc tả cho các giao diện giữa các TOE thành phần và thiết kế TOE (mô tả các mô đun TSF) được chứa trong thông tin phát triển tổng hợp để hiểu về hành vi an toàn.

Phân tích được hỗ trợ bằng cách kiểm tra độc lập của các giao diện của thành phần cơ sở được dựa trên thành phần phụ thuộc, như mô tả trong thông tin tin cậy (nay bao gồm cả thiết kế TOE), kiểm tra chứng cứ của nhà phát triển dựa trên thông tin tin cậy, thông tin phát triển và sở cứ tổng hợp và chọn lọc độc lập xác nhận kết quả kiểm thử của nhà phát triển. Phân tích này cũng được hỗ trợ với việc phân tích điểm yếu của TOE tổng hợp bởi đánh giá viên để chứng minh khả năng chống kẻ tấn công với khả năng tấn công trên mức cơ bản.

CAP này thể hiện sự gia tăng có ý nghĩa trong sự bảo đảm từ CAP-B bằng cách yêu cầu mô tả chi tiết thiết kế và thể hiện khả năng chống lại khả năng bị tấn công cao hơn.

Bảng 12 – CAP-C

Lớp đảm bảo	Các thành phần đảm bảo
ACO: Thành phần cấu tạo	ACO_COR.1 Sở cứ tổng hợp
	ACO_CTT.2 Kiểm thử giao diện nghiêm ngặt
	ACO_DEV.3: Chứng cứ chi tiết cho thiết kế
	ACO_REL.2: Thông tin tin cậy
	ACO_VUL.3: Phân tích điểm yếu tổng hợp mức cao hơn cơ bản

AGD: Tài liệu hướng dẫn	AGD_OPE.1 Hướng dẫn người dùng vận hành
	AGD_PRE.1 Các thủ tục chuẩn bị
ALC: Hỗ trợ vòng đời	ACL_CMC.1 Gắn nhãn cho TOE
	ACL_CMS.2: Các phần của TOE CM tổng quát
Đánh giá các đích an toàn	ASE_CCL.1 Các yêu cầu tuân thủ
	ASE_ECD.1 Định nghĩa các thành phần mở rộng
	ASE_INT.1: Giới thiệu ST
	ASE_OBJ.2: Các mục tiêu an toàn
	ASE_REQ.2: Các yêu cầu an toàn được cung cấp
	ASE_SPD.1 Định nghĩa các vấn đề an toàn
	ASE_TSS.1: Đặc tả tổng quát TOE

9 Lớp APE: Đánh giá hồ sơ bảo vệ

Đánh giá một PP được yêu cầu để chứng minh rằng PP là nhất quán và nếu là PP dựa trên một hoặc nhiều PP khác hoặc trong các gói, mà PP là một thể hiện đúng của các PP này và các gói. Các thuộc tính này là cần thiết cho PP cho phù hợp để sử dụng làm cơ sở để viết ST hay PP khác.

Mục này nên được sử dụng cùng với các Phụ lục A, B và C trong TCVN 8709-1, như các phụ lục để làm rõ các khái niệm ở đây và cung cấp nhiều ví dụ.

Hình 8 cho thấy các họ trong lớp này, và hệ thống phân cấp của các thành phần trong họ.

Hình 8 - Phân cấp lớp APE: Đánh giá Hồ sơ bảo vệ

9.1 Giới thiệu PP (APE_INT)

9.1.1 Mục tiêu

Mục tiêu của họ này là mô tả TOE theo một phạm vi hẹp.

Đánh giá giới thiệu PP được đòi hỏi để chứng minh rằng PP được xác định đúng và tham chiếu PP và tổng quan TOE là nhất quán với các thành phần khác.

9.1.2 APE_INT.1 Giới thiệu PP

Các mối phụ thuộc: không có sự phụ thuộc nào.

9.1.2.1 Phần tử hành động của nhà phát triển

9.1.2.1.1 APE_INT.1.1D

Nhà phát triển PP cần cung cấp giới thiệu PP

9.1.2.2 Các phần tử nội dung và trình bày

9.1.2.2.1 APE_INT.1.1C

Giới thiệu PP cần chứa tham chiếu PP và tổng quan TOE

9.1.2.2.2 APE_INT.1.2C

Tham chiếu PP cần là định danh duy nhất của PP

9.1.2.2.3 APE_INT.1.3C

Tổng quan TOE cần tóm tắt việc sử dụng và các đặc trưng an toàn chính của TOE

9.1.2.2.4 APE_INT.1.4C

Tổng quan TOE cần xác định kiểu TOE.

9.1.2.2.5 APE_INT_1.5C

Tổng quan TOE cần xác định bất kỳ phần cứng, phần mềm và phần sụn không phải TOE có trong TOE.

9.1.2.3 Các phần tử hành động của đánh giá viên

9.1.2.3.1 APE_INT.1.1E

Đánh giá viên cần khẳng định rằng thông tin cung cấp đáp ứng mọi yêu cầu về chứng cứ cho nội dung và trình bày.

9.2 Các yêu cầu tuân thủ (APE_CCL)

9.2.1 Mục tiêu

Mục tiêu của họ này là quyết định giá trị của các yêu cầu tuân thủ. Thêm vào đó, họ này chỉ ra làm sao mà ST và các PP khác được yêu cầu tuân thủ với PP.

9.2.2 APE_CCL.1 Các yêu cầu tuân thủ

Các phụ thuộc: APE_INT.1 Giới thiệu PP

APE_ECD.1 Định nghĩa các thành phần mở rộng

APE_REQ.1 Nêu các yêu cầu an toàn.

9.2.2.1 Phần tử hành động của nhà phát triển

9.2.2.1.1 APE_CCL.1.1D

Nhà phát triển cần cung cấp yêu cầu tuân thủ

9.2.2.1.2 APE_CCL.1.2D

Nhà phát triển cần cung cấp sở cứ các yêu cầu tuân thủ

9.2.2.1.3 APE_CCL.1.3D

Nhà phát triển cần cung cấp các tuyên bố về tuân thủ

9.2.2.2 Các phần tử nội dung và trình bày

9.2.2.2.1 APE_CCL.1.1C

Các yêu cầu tuân thủ cần chứa yêu cầu tuân thủ TCVN 8709 mà xác định phiên bản của TCVN 8709 mà PP yêu cầu tuân thủ.

9.2.2.2.2 APE_CCL.1.2C

Các yêu cầu tuân thủ TCVN 8709 cần mô tả sự tuân thủ của PP theo TCVN 8709-2 cũng như là sự tuân thủ TCVN 8709-2 hoặc mở rộng của TCVN 8709-2.

9.2.2.2.3 APE_CCL.1.3C

Các yêu cầu tuân thủ TCVN 8709 cần mô tả sự tuân thủ của PP theo phần này của TCVN 8709 cũng như là sự tuân thủ phần này của TCVN 8709 hoặc phần này của phần mở rộng TCVN 8709.

9.2.2.2.4 APE_CCL.1.4C

Yêu cầu tuân thủ TCVN 8709 cần nhất quán với định nghĩa các thành phần mở rộng

9.2.2.2.5 APE_CCL.1.5C

Yêu cầu tuân thủ TCVN 8709 cần chỉ ra tất cả PP và các gói yêu cầu an toàn mà PP yêu cầu tuân thủ.

9.2.2.2.6 APE_CCL.1.6C

Yêu cầu tuân thủ cần mô tả bất kỳ sự tuân thủ nào của PP theo gói cũng như gói tuân thủ hay gói tăng cường khác.

9.2.2.2.7 APE_CCL.1.7C

Sở cứ cho yêu cầu tuân thủ cần chứng minh rằng kiểu TOE này là nhất quán với kiểu TOE trong các PP mà sự tuân thủ đang được yêu cầu.

9.2.2.2.8 APE_CCL.1.8C

Sở cứ cho yêu cầu tuân thủ sẽ chứng minh rằng tuyên bố định nghĩa các vấn đề an toàn là nhất quán với tuyên bố về định nghĩa các vấn đề an toàn bên trong các PP mà sự tuân thủ đang được yêu cầu.

9.2.2.2.9 APE_CCL.1.9C

Sở cứ cho yêu cầu tuân thủ cần chứng minh rằng tuyên bố các mục tiêu an toàn là nhất quán với tuyên bố về định nghĩa các mục tiêu an toàn bên trong các PP mà sự tuân thủ đang được yêu cầu.

9.2.2.2.10 APE_CCL.1.10C

Sở cứ cho yêu cầu tuân thủ cần chứng minh rằng tuyên bố định nghĩa các yêu cầu an toàn là nhất quán với tuyên bố về định nghĩa các yêu cầu an toàn bên trong các PP mà sự tuân thủ đang được yêu cầu.

9.2.2.2.11 APE_CCL.1.11C

Tuyên bố tuân thủ cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

9.2.2.3 Các phần tử hành động của đánh giá viên

9.2.2.3.1 APE_CCL.1.1E

Đánh giá viên cần khẳng định rằng thông tin cung cấp đáp ứng mọi yêu cầu về chứng cứ cho nội dung và trình bày.

9.3 Định nghĩa vấn đề an toàn (APE_SPD)

9.3.1 Mục tiêu

Phần này của PP định nghĩa các vấn đề an toàn được đề cập đến trong TOE và môi trường áp dụng của TOE.

Đánh giá định nghĩa các vấn đề an toàn được yêu cầu để chứng minh rằng các vấn đề an toàn dự kiến được đề cập bởi TOE và môi trường áp dụng của nó, được định nghĩa rõ ràng.

9.3.2 APE_SPD.1 định nghĩa các vấn đề an toàn

Các mối phụ thuộc: không có sự phụ thuộc nào

9.3.2.1 Phần tử hành động của nhà phát triển

9.3.2.1.1 APE_SPD.1.1D

Nhà phát triển cần cung cấp định nghĩa các vấn đề an toàn

9.3.2.2 Nội dung và trình bày của các thành phần

9.3.2.2.1 APE_SPD.1.1C

Định nghĩa các vấn đề an toàn cần mô tả các mối đe dọa.

9.3.2.2.2 APE_SPD.1.2C

Tất cả các mối đe dọa cần được mô tả dưới dạng tác nhân gây nguy cơ, tài sản và các hành động thù địch.

9.3.2.2.3 APE_SPD.1.3C

Định nghĩa vấn đề an toàn cần mô tả các OSP.

9.3.2.2.4 APE_SPD.1.4C

Định nghĩa các vấn đề an toàn cần mô tả giả thiết về môi trường vận hành của TOE.

9.3.2.3 Các phần tử hành động của đánh giá viên

9.3.2.3.1 APE_SPD.1.1E

Đánh giá viên cần khẳng định rằng thông tin cung cấp đáp ứng mọi yêu cầu về chứng cứ cho nội dung và trình bày.

9.4 Các mục tiêu an toàn (APE_OBJ)

9.4.1 Mục tiêu

Các mục tiêu an toàn là tuyên bố ngắn gọn của phản ứng dự định cho vấn đề an toàn được định nghĩa thông qua định nghĩa các vấn đề an toàn (họ APE_SPD).

Đánh giá các mục tiêu an toàn được đòi hỏi để chứng minh rằng các mục tiêu an toàn được đề cập đến là tương xứng và đầy đủ cho các vấn đề an toàn và sự phân tách giữa TOE và môi trường áp dụng nó sẽ được định nghĩa rõ ràng.

9.4.2 Phân mức thành phần

Các thành phần trong họ này được phân mức ra dựa trên việc quy định chúng là mục tiêu an toàn cho môi trường áp dụng hay mục tiêu an toàn cho TOE.

9.4.3 APE_OBJ.1 Các mục tiêu an toàn cho môi trường áp dụng

Các mối phụ thuộc: không có sự phụ thuộc nào.

9.4.3.1 Phần tử hành động của nhà phát triển

9.4.3.1.1 APE_OBJ.1.1D

Nhà phát triển PP cần cung cấp tuyên bố các mục tiêu an toàn.

9.4.3.2 Các phần tử nội dung và trình bày

9.4.3.2.1 APE_OBJ.1.1C

Tuyên bố các mục tiêu an toàn cần mô tả các mục tiêu an toàn cho môi trường vận hành.

9.4.3.3 Các phần tử hành động của đánh giá viên

9.4.3.3.1 APE_OBJ.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày các chứng cứ.

9.4.4 APE_OBJ.2 Các mục tiêu an toàn

Các phụ thuộc: APE_SPD.1 định nghĩa vấn đề an toàn

9.4.4.1 Phần tử hành động của nhà phát triển

9.4.4.1.1 APE_OBJ.2.1D

Nhà phát triển cần cung cấp tuyên bố về các mục tiêu an toàn

9.4.4.1.2 APE_OBJ.2.2D

Nhà phát triển cần cung cấp sở cứ cho các mục tiêu an toàn.

9.4.4.2 Các phần tử nội dung và trình bày

9.4.4.2.1 APE_OBJ.2.1C

Tuyên bố về mục tiêu an toàn cần mô tả các mục tiêu an toàn cho TOE và các mục tiêu an toàn cho môi trường áp dụng.

9.4.4.2.2 APE_OBJ.2.2C

Sở cứ các mục tiêu an toàn cần theo vết từng mục tiêu an toàn cho TOE chống lại các nguy cơ bởi các mục tiêu an toàn đó và các OSP được thực hiện bởi các mục tiêu an toàn.

9.4.4.2.3 APE_OBJ.2.3C

Sở cứ các mục tiêu an toàn cần theo vết từng mục tiêu an toàn cho môi trường áp dụng chống lại các nguy cơ bởi các mục tiêu an toàn đó và các OSP được thực hiện bởi các mục tiêu an toàn và giả định duy trì các mục tiêu an toàn.

9.4.4.2.4 APE_OBJ.2.4C

Sở cứ các mục tiêu an toàn cần chứng minh rằng các mục tiêu an toàn chống lại tất cả các nguy cơ.

9.4.4.2.5 APE_OBJ.2.5C

Sở cứ các mục tiêu an toàn cần chứng minh rằng các mục tiêu an toàn thực thi tất cả OSP.

9.4.4.2.6 APE_OBJ.2.6C

Sở cứ các mục tiêu an toàn cần chứng minh rằng các mục tiêu an toàn cho môi trường áp dụng duy trì tất cả các giả định.

9.4.4.3 Các phần tử hành động của đánh giá viên

9.4.4.3.1 APE_OBJ.2.1E

Đánh giá viên cần xác nhận rằng các thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

9.5 Định nghĩa các thành phần mở rộng (APE_ECD)

9.5.1 Mục tiêu

Các yêu cầu an toàn mở rộng là các yêu cầu mà không dựa trên các thành phần từ TCVN 8709-2 hay phần này của TCVN 8709 mà dựa trên các thành phần mở rộng : các thành phần được định nghĩa bởi tác giả PP.

Đánh giá định nghĩa các thành phần mở rộng là cần thiết để quyết định rằng chúng rất rõ ràng và không mập mờ, và chúng là cần thiết, ví dụ chúng không thể được biểu diễn rõ ràng nếu sử dụng các thành phần đang có trong TCVN 8709-2 hoặc phần này của TCVN 8709

9.5.2 APE_ECD.1 định nghĩa các thành phần mở rộng

Các mối phụ thuộc: không có sự phụ thuộc nào.

9.5.2.1 Phần tử hành động của nhà phát triển

9.5.2.1.1 APE_ECD.1.1D

Nhà phát triển cần cung cấp tuyên bố về các yêu cầu an toàn

9.5.2.1.2 APE_ECD.1.2D

Nhà phát triển cần cung cấp định nghĩa các thành phần mở rộng

9.5.2.2 Các phần tử nội dung và trình bày

9.5.2.2.1 APE_ECD.1.1C

Tuyên bố các yêu cầu an toàn cần xác định tất cả các yêu cầu an toàn mở rộng.

9.5.2.2.2 APE_ECD.1.2C

Định nghĩa các thành phần mở rộng cần xác định thành phần mở rộng cho từng yêu cầu an toàn mở rộng.

9.5.2.2.3 APE_ECD.1.3C

Định nghĩa các thành phần mở rộng cần được mô tả mỗi thành phần mở rộng có quan hệ thế nào với các lớp, họ và thành phần đang có trong TCVN 8709.

9.5.2.2.4 APE_ECD.1.4C

Định nghĩa các thành phần mở rộng cần sử dụng các lớp, họ, thành phần của TCVN 8709 đang tồn tại như là mô hình cho sự trình bày.

9.5.2.2.5 APE_ECD.1.5C

Các thành phần mở rộng cần sử dụng phương pháp, lớp, họ và thành phần đang có trong TCVN 8709 như là mô hình trong sự trình bày.

9.5.2.3 Các phần tử hành động của đánh giá viên

9.5.2.3.1 APE_ECD.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày của các chứng cứ.

9.5.2.3.2 APE_ECD.1.2E

đánh giá viên **cần xác nhận rằng không thành phần mở rộng nào được biểu diễn rõ ràng sử dụng các thành phần đang tồn tại.**

9.6 Các yêu cầu an toàn (APE_REQ)

9.6.1 Mục tiêu

SFR được mô tả một cách rõ ràng, không lẫn lộn được xác định hoàn toàn các hành vi an toàn mong muốn của TOE. SAR được mô tả một cách rõ ràng, không lẫn lộn được hoàn toàn xác định các hoạt động mong muốn mà có trách nhiệm đạt được sự đảm bảo trong TOE.

Đánh giá các yêu cầu an toàn được yêu cầu để đảm bảo rằng chúng là rõ ràng, không lẫn lộn và được hoàn toàn xác định.

9.6.2 Phân mức thành phần

Các thành phần trong họ này được phân mức mà chúng được quy định hay SFR được bắt nguồn từ các mục tiêu an toàn cho TOE.

9.6.3 APE_REQ.1 Các yêu cầu an toàn được tuyên bố

Các phụ thuộc: APE_ECD.1 Định nghĩa các thành phần mở rộng

9.6.3.1 Phần tử hành động của nhà phát triển

9.6.3.1.1 APE_REQ.1.1D

Nhà phát triển cần cung cấp tuyên bố về các yêu cầu an toàn

9.6.3.1.2 APE_REQ.1.2D

Nhà phát triển cần cung cấp các sở cứ về các yêu cầu an toàn

9.6.3.2 Các phần tử nội dung và trình bày

9.6.3.2.1 APE_REQ.1.1C

Tuyên bố về các yêu cầu an toàn cần mô tả các SFR và SAR

9.6.3.2.2 APE_REQ.1.2C

Tất cả các đối tượng, mục tiêu, hoạt động, thuộc tính an toàn, các thực thể bên ngoài và các nhóm khác được sử dụng trong SFR và SAR, cần được xác định.

9.6.3.2.3 APE_REQ.1.3C

Tuyên bố về các yêu cầu an toàn cần xác định tất cả các quá trình hoạt động trong các yêu cầu an toàn.

9.6.3.2.4 APE_REQ.1.4C

Tất cả các hoạt động cần phải thực hiện đúng

9.6.3.2.5 APE_REQ.1.5C

Mỗi phụ thuộc của các yêu cầu an toàn không chỉ cần được thỏa mãn mà sở cứ các yêu cầu an toàn cần phải biện minh cho các phụ thuộc không được thỏa mãn.

9.6.3.2.6 APE_REQ.1.6C

Tuyên bố về các yêu cầu an toàn cần phải có tính nhất quán nội bộ.

9.6.3.3 Các phần tử hành động của đánh giá viên

9.6.3.3.1 APE_REQ.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày của các chứng cứ.

9.6.4 APE_REQ.2 Các yêu cầu an toàn thu được

Các phụ thuộc: APE_OBJ.2 Các mục tiêu an toàn

APE_ECD.1 Định nghĩa các thành phần mở rộng

9.6.4.1 Phần tử hành động của nhà phát triển

9.6.4.1.1 APE_REQ.2.1D

Nhà phát triển cần cung cấp tuyên bố về các yêu cầu an toàn

9.6.4.1.2 APE_REQ.2.2D

Nhà phát triển cần cung cấp sở cứ các yêu cầu an toàn.

9.6.4.2 Các phần tử nội dung và trình bày

9.6.4.2.1 APE_REQ.2.1C

Tuyên bố các yêu cầu an toàn cần mô tả SFR và SAR.

9.6.4.2.2 APE_REQ.2.2C

Tất cả các đối tượng, mục tiêu, hoạt động, thuộc tính an toàn, các thực thể bên ngoài và các nhóm khác được sử dụng trong SFR và SAR, cần được xác định.

9.6.4.2.3 APE_REQ.2.3C

Tuyên bố về các yêu cầu an toàn cần xác định tất cả các quá trình hoạt động trong các yêu cầu an toàn.

9.6.4.2.4 APE_REQ.2.4C

Các hoạt động cần phải được thực hiện đúng

9.6.4.2.5 APE_REQ.2.5C

Mỗi phụ thuộc của các yêu cầu an toàn không chỉ cần được thỏa mãn mà sở cứ các yêu cầu an toàn cần phải biện minh cho các phụ thuộc không được thỏa mãn.

9.6.4.2.6 APE_REQ.2.6C

Sở cứ các yêu cầu an toàn cần theo vết mỗi SFR quay lại các mục tiêu an toàn cho TOE.

9.6.4.2.7 APE_REQ.2.7C

Sở cứ các yêu cầu an toàn cần chứng minh rằng SFR đáp ứng tất cả các mục tiêu an toàn cho TOE.

9.6.4.2.8 APE_REQ.2.8C

Sở cứ các yêu cầu an toàn cần giải thích vì sao các SAP được chọn.

9.6.4.2.9 APE_REQ.2.9C

Tuyên bố về các yêu cầu an toàn cần nhất quán nội bộ

9.6.4.3 Các phần tử hành động của đánh giá viên

9.6.4.3.1 APE_REQ.2.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày các chứng cứ.

10 Lớp ASE: Đánh giá đích an toàn

Mục tiêu của đánh giá ST là chứng minh rằng ST đó đã hoàn tất, nhất quán, phù hợp và nếu ST được dựa trên một hoặc nhiều PP hay các gói, khi đó ST là một thể hiệu đúng của các PP và các gói này. Các thuộc tính này là cần thiết cho ST để phù hợp cho sử dụng như là cơ sở cho đánh giá TOE.

Phần này cần được kết nối với các Phụ lục A, B và C trong TCVN 8709-1, phụ lục này làm rõ các khái niệm ở đây và cung cấp nhiều ví dụ.

Hình 9 chỉ ra các họ bên trọng lớp này và phân cấp các thành phần trong các họ này.

Hình 9 – Phân cấp lớp ASE: Đánh giá Đích an toàn

10.1 Giới thiệu ST (ASE_INT)

10.1.1 Mục tiêu

Mục tiêu của họ này là mô tả TOE theo một cách hẹp theo ba mức gồm : Tham chiếu TOE, Tổng quan TOE và mô tả TOE.

Đánh giá giới thiệu ST được yêu cầu để chứng minh rằng ST và TOE được xác định đúng, do đó TOE được mô tả đúng tại 3 mức và mô tả của 3 mức này nhất quán với mỗi cái khác.

10.1.2 ASE_INT.1 Giới thiệu ST

Các mối phụ thuộc: không có sự phụ thuộc nào.

10.1.2.1 Phần tử hành động của nhà phát triển

10.1.2.1.1 ASE_INT.1.1D

Nhà phát triển cần cung cấp giới thiệu ST.

10.1.2.2 Các phần tử nội dung và trình bày

10.1.2.2.1 ASE_INT.1.1C

Giới thiệu ST cần chứa tham chiếu ST, tham chiếu TOE, tổng quan TOE và mô tả TOE.

10.1.2.2.2 ASE_INT.1.2C

Tham chiếu ST cần xác định ST duy nhất.

10.1.2.2.3 ASE_INT.1.3C

Tham chiếu TOE cần xác định TOE.

10.1.2.2.4 ASE_INT.1.4C

Tổng quan TOE cần tóm tắt việc sử dụng các đặc trưng an toàn chính của TOE.

10.1.2.2.5 ASE_INT.1.5C

Tổng quan TOE cần xác định kiểu TOE.

10.1.2.2.6 ASE_INT.1.6C

Tổng quan TOE cần xác định bất kỳ phần cứng, phần mềm, phần sụn nào không phải TOE được yêu cầu bởi TOE.

10.1.2.2.7 ASE_INT.1.7C

Mô tả TOE cần mô tả phạm vi vật lý của TOE.

10.1.2.2.8 ASE_INT.1.8C

Mô tả TOE cần mô tả phạm vi logic của TOE.

10.1.2.3 Phần tử hành động của đánh giá viên

10.1.2.3.1 ASE_INT.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày của chứng cứ.

10.1.2.3.2 ASE_INT.1.2E

Đánh giá viên cần xác nhận rằng tham chiếu TOE, tổng quan TOE và mô tả TOE là nhất quán với các cái khác.

10.2 Các yêu cầu tuân thủ (ASE_CCL)

10.2.1 Mục tiêu

Mục tiêu của họ này là quyết định giá trị của yêu cầu tuân thủ. Thêm vào đó, họ này chỉ ra làm thế nào các ST yêu cầu tuân thủ với PP.

10.2.2 ACE_CCL.1 Các yêu cầu tuân thủ

Các phụ thuộc: ASE_INT.1 ST Giới thiệu

ASE_ECD.1 Định nghĩa các thành phần mở rộng

ASE_REQ.1 Tuyên bố về các yêu cầu an toàn

10.2.2.1 Các phần tử hành động của đánh giá viên

10.2.2.1.1 ASE_CCL.1.1D

Nhà phát triển cần cung cấp yêu cầu tuân thủ

10.2.2.1.2 ASE_CCL.1.2D

Nhà phát triển cần cung cấp sở cứ yêu cầu tuân thủ

10.2.2.2 Các phần tử nội dung và trình bày

10.2.2.2.1 ASE_CCL.1.1C

Yêu cầu tuân thủ cần chứa yêu cầu tuân thủ TCVN 8709 để xác định phiên bản của TCVN 8709-2 mà yêu cầu tuân thủ TOE và ST.

10.2.2.2.2 ASE_CCL.1.2C

Yêu cầu tuân thủ TCVN 8709 cần mô tả tuân thủ của ST theo TCVN 8709-2, không chỉ tuân thủ TCVN 8709-2 mà còn TCVN 8709-2 mở rộng.

10.2.2.2.3 ASE_CCL.1.3C

Yêu cầu tuân thủ TCVN 8709 cần mô tả tuân thủ của ST theo phần này của TCVN 8709 không chỉ tuân thủ theo phần này của TCVN 8709 mà còn theo phần này của TCVN 8709 mở rộng.

10.2.2.2.4 ASE_CCL.1.4C

Yêu cầu tuân thủ TCVN 8709 cần nhất quán với định nghĩa các thành phần mở rộng.

10.2.2.2.5 ASE_CCL.1.5C

Yêu cầu tuân thủ cần chỉ ra tất cả các PP và các gói đảm bảo an toàn mà ST yêu cầu tuân thủ.

10.2.2.2.6 ASE_CCL.1.6C

Yêu cầu tuân thủ cần mô tả bất kỳ tuân thủ nào của ST theo gói, không chỉ các gói tuân thủ mà cả các gói tăng cường.

10.2.2.2.7 ASE_CCL.1.7C

Sở cứ yêu cầu tuân thủ cần chứng minh rằng kiểu TOE là nhất quán với kiểu TOE trong PP theo đó sự tuân thủ được yêu cầu.

10.2.2.2.8 ASE_CCL.1.8C

Sở cứ yêu cầu tuân thủ cần chứng minh rằng tuyên bố của định nghĩa vấn đề an toàn là nhất quán với tuyên bố định nghĩa các vấn đề an toàn trong PP theo đó sự tuân thủ được yêu cầu.

10.2.2.2.9 ASE_CCL_1.9C

Sở cứ yêu cầu tuân thủ cần chứng minh rằng các tuyên bố của mục tiêu an toàn là nhất quán với tuyên bố của mục tiêu an toàn trong PP theo đó sự tuân thủ được yêu cầu.

10.2.2.2.10 ASE_CCL.1.10C

Sở cứ các yêu cầu tuân thủ cần chứng minh rằng tuyên bố của các yêu cầu an toàn là nhất quán với tuyên bố của các yêu cầu an toàn trong PP mà tại đó sự tuân thủ được yêu cầu.

10.2.2.3 Các phần tử hành động của đánh giá viên

10.2.2.3.1 ASE_CCL.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và biểu diễn các chứng cứ.

10.3 Định nghĩa vấn đề an toàn (ASE_SPD)

10.3.1 Mục tiêu

Trong phần này của ST định nghĩa vấn đề an toàn được đề cập bởi TOE và môi trường áp dụng TOE.

Đánh giá định nghĩa các vấn đề an toàn được yêu cầu để chứng minh rằng vấn đề an toàn dự định được đề cập bởi TOE và môi trường áp dụng của nó là được định nghĩa rõ ràng.

10.3.2 ASE_SPD.1 Định nghĩa vấn đề an toàn

Các mối phụ thuộc: không có sự phụ thuộc nào.

10.3.2.1 Phần tử hành động của nhà phát triển

10.3.2.1.1 ASE_SPD.1.1D

Nhà phát triển cần cung cấp định nghĩa các vấn đề an toàn

10.3.2.2 Các phần tử nội dung và trình bày

10.3.2.2.1 ASE_SPD.1.1C

Định nghĩa vấn đề an toàn cần mô tả các nguy cơ

10.3.2.2.2 ASE_SPD.1.2C

Tất cả các nguy cơ cần mô tả dưới dạng tác nhân nguy cơ, tài sản và hành động bất lợi.

10.3.2.2.3 ASE_SPD.1.3C

Định nghĩa vấn đề an toàn cần mô tả OSP

10.3.2.2.4 ASE_SPD.1.4C

Định nghĩa vấn đề an toàn cần mô tả giả thiết về môi trường hoạt động của TOE.

10.3.2.3 Các phần tử hành động của đánh giá viên

10.3.2.3.1 ASE_SPD.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày của các chứng cứ.

10.4 Mục tiêu an toàn (ASE_OBJ)

10.4.1 Mục tiêu

Các mục tiêu an toàn là tuyên bố ngắn gọn của các phản ứng dự định cho các vấn đề về an toàn được định nghĩa qua định nghĩa các vấn đề an toàn của họ (ASE_SPD)

Đánh giá các mục tiêu an toàn được yêu cầu để chứng minh rằng các mục tiêu an toàn là phù hợp và đề cập hoàn toàn đến định nghĩa các vấn đề an toàn mà sự phân chia của vấn đề này giữa TOE và môi trường hoạt động của nó được định nghĩa rõ ràng.

10.4.2 Phân mức thành phần

Các thành phần trong họ này được phân mức dựa trên có hay không việc quy định chỉ các mục tiêu an toàn cho môi trường áp dụng hay cả các mục tiêu an toàn cho TOE.

10.4.3 ASE_OBJ.1 Các mục tiêu an toàn cho môi trường hoạt động

Các mối phụ thuộc: không có sự phụ thuộc nào.

10.4.3.1 Phần tử hành động của nhà phát triển.

10.4.3.1.1 ASE_OBJ.1.1D

Nhà phát triển cần cung cấp tuyên bố về mục tiêu an toàn

10.4.3.2 Các phần tử nội dung và trình bày

10.4.3.2.1 ASE_OBJ.1.1C

Tuyên bố về các mục tiêu an toàn cần mô tả các mục tiêu an toàn cho môi trường áp dụng

10.4.3.3 Các phần tử hành động của đánh giá viên

10.4.3.3.1 ASE_OBJ.1.1E

Đánh giá viên cần xác nhận rằng các thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và biểu diễn các chứng cứ.

10.4.4 ASE_OBJ.2 Các mục tiêu an toàn.

Các phụ thuộc: ASE_SPD.1 định nghĩa các vấn đề an toàn

10.4.4.1 Phần tử hành động của nhà phát triển

10.4.4.1.1 ASE_OBJ.2.1D

Nhà phát triển cần cung cấp tuyên bố về các mục tiêu an toàn.

10.4.4.1.2 ASE_OBJ.2.2D

Nhà phát triển cần cung cấp sở cứ các mục tiêu an toàn

10.4.4.2 Các phần tử nội dung và trình bày

10.4.4.2.1 ASE_OBJ.2.1C

Tuyên bố về các mục tiêu an toàn cần mô tả các mục tiêu an toàn cho TOE và các mục tiêu an toàn cho môi trường áp dụng.

10.4.4.2.2 ASE_OBJ.2.2C

Sở cứ các mục tiêu an toàn cần theo vết mỗi mục tiêu an toàn cho TOE trở lại chống lại các nguy cơ bởi mục tiêu an toàn đó và thực thi OSP bởi mục tiêu an toàn đó.

10.4.4.2.3 ASE_OBJ.2.3C

Sở cứ các mục tiêu an toàn cần theo vết mỗi mục tiêu an toàn cho môi trường áp dụng trở lại chống lại các nguy cơ bởi mục tiêu an toàn đó, thực thi OSP bởi mục tiêu an toàn đó, và giả thiết duy trì mục tiêu an toàn đó.

10.4.4.2.4 ASE_OBJ.2.4C

Sở cứ các mục tiêu an toàn cần chứng minh rằng mục tiêu an toàn chống lại tất cả các nguy cơ.

10.4.4.2.5 ASE_OBJ.2.5C

Sở cứ các mục tiêu an toàn cần chứng minh rằng mục tiêu an toàn chống lại tất cả các OSP.

10.4.4.2.6 ASE_OBJ.2.6C

Sở cứ các mục tiêu an toàn cần chứng minh rằng mục tiêu an cho môi trường áp dụng duy trì tất cả các giả thiết.

10.4.4.3 Các phần tử hành động của đánh giá viên

10.4.4.3.1 ASE_OBJ.2.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp cần đáp ứng tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

10.5 Định nghĩa các thành phần mở rộng (ASE_ECD)

10.5.1 Mục tiêu

Các yêu cầu an toàn mở rộng là các yêu cầu mà không dựa trên các thành phần từ TCVN 8709-2 hay phần này của TCVN 8709, mà dựa trên các thành phần mở rộng: Thành phần được định nghĩa bởi tác giả ST.

Đánh giá định nghĩa các thành phần mở rộng cần thiết để quyết định rằng chúng là rõ ràng và không thể nhầm lẫn, và do đó chúng là cần thiết, ví dụ chúng có thể không được biểu diễn rõ ràng sử dụng TCVN 8709-2 hoặc phần này của các thành phần TCVN 8709.

10.5.2 ASE_ECD.1 Định nghĩa các thành phần mở rộng

Các mối phụ thuộc: không có sự phụ thuộc nào.

10.5.2.1.1 ASE_ECD.1.1D

Nhà phát triển cần cung cấp tuyên bố về yêu cầu an toàn.

10.5.2.1.2 ASE_ECD.1.2D

Nhà phát triển cần cung cấp định nghĩa các thành phần mở rộng.

10.5.2.2 Các phần tử nội dung và trình bày

10.5.2.2.1 ASE_ECD.1.1C

Tuyên bố các yêu cầu an toàn cần xác định tất cả các yêu cầu an toàn mở rộng.

10.5.2.2.2 ASE_ECD.1.2C

Định nghĩa các thành phần mở rộng cần định nghĩa thành phần mở rộng cho mỗi yêu cầu an toàn mở rộng.

10.5.2.2.3 ASE_ECD.1.3C

Định nghĩa các thành phần mở rộng cần mô tả mỗi thành phần mở rộng có mối quan hệ như thế nào với các thành phần, họ và lớp trong TCVN 8709 đang tồn tại.

10.5.2.2.4 ASE_ECD.1.4C

Định nghĩa các thành phần mở rộng cần sử dụng các thành phần, lớp, họ và phương pháp trong TCVN 8709 như một mô hình cho trình bày.

10.5.2.3 Các phần tử hành động của đánh giá viên

10.5.2.3.1 ASE_ECD.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày của chứng cứ.

10.5.2.3.2 ASE_ECD.1.2E

Đánh giá viên cần xác nhận rằng không thành phần mở rộng nào có thể biểu diễn rõ ràng mà sử dụng các thành phần đang có.

10.6 Các yêu cầu an toàn (ASE_REQ)

10.6.1 Mục tiêu

SFR được mô tả một cách rõ ràng, không lẫn lộn được xác định hoàn toàn các hành vi an toàn mong muốn của TOE. SAR được mô tả một cách rõ ràng, không lẫn lộn được hoàn toàn xác định các hoạt động mong muốn mà có trách nhiệm đạt được sự đảm bảo trong TOE.

Đánh giá các yêu cầu an toàn được yêu cầu để đảm bảo rằng chúng là rõ ràng, không lẫn lộn và được hoàn toàn xác định.

10.6.2 Phân mức thành phần

Các thành phần trong họ này được phân mức theo như chúng được tuyên bố.

10.6.3 ASE_REQ.1 Định nghĩa các thành phần mở rộng

10.6.3.1 Phần tử hành động của nhà phát triển.

10.6.3.1.1 ASE_REQ.1.1D

Nhà phát triển cần cung cấp tuyên bố về yêu cầu an tòan

10.6.3.1.2 ASE_REQ.1.2D

Nhà phát triển cần cung cấp sờ cứ các yêu cầu an toàn

10.6.3.2 Các phần tử nội dung và trình bày

10.6.3.2.1 ASE_REQ.1.1C

Tuyên bố các yêu cầu an toàn cần mô tả SFR và SAR

10.6.3.2.2 ASE_REQ.1.2C

Tất cả các chủ thể, mục tiêu, hoạt động, thuộc tính an toàn, thực thể ngoài và các thuật ngữ các được sử dụng trong SFR và SAR cần được định nghĩa.

10.6.3.2.3 ASE_REQ.1.3C

Tuyên bố về các yêu cầu an toàn cần xác định tất cả các hoạt động dựa trên các yêu cầu an toàn.

10.6.3.2.4 ASE_REQ.1.4C

Tất cả các hoạt động cần thực hiện chính xác.

10.6.3.2.5 ASE_REQ.1.5C

Mỗi các mối phụ thuộc của các yêu cầu an toàn cần không chỉ sự thỏa mãn mà sở cứ các yêu cầu an toàn cần biện minh cho các mối phụ thuộc không được thỏa mãn.

10.6.3.2.6 ASE_REQ.1.6C

Tuyên bố về các yêu cầu an toàn cần nhất quán nội bộ.

10.6.3.3 Các phần tử hành động của đánh giá viên

10.6.3.3.1 ASE_REQ.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

10.6.4 ASE_REQ.2 Các yêu cầu an toàn thu được

Các phụ thuộc: ASE_OBJ.2 Các mục tiêu an toàn

ASE_ECD.1 Định nghĩa các thành phần mở rộng

10.6.4.1 Phần tử hành động của nhà phát triển

10.6.4.1.1 ASE_REQ.2.1D

Nhà phát triển cần cung cấp tuyên bố các yêu cầu an toàn.

10.6.4.1.2 ASE_REQ.2.2D

Nhà phát triển cần cung cấp sở cứ các yêu cầu an toàn.

10.6.4.2 Các phần tử nội dung và trình bày

10.6.4.2.1 ASE_REQ.2.1C

Tuyên bố các yêu cầu an toàn cần mô tả SFR và SAR.

10.6.4.2.2 ASE_REQ.2.2C

Tất cả các chủ thể, mục tiêu, hoạt động, thuộc tính an toàn, thực thể ngoài và các thuật ngữ được sử dụng trong SFR và SAR cần được định nghĩa.

10.6.4.2.3 ASE_REQ.2.3C

Tuyên bố các yêu cầu an toàn cần chỉ ra tất cả các hoạt động dựa trên các yêu cầu an toàn.

10.6.4.2.4 ASE_REQ.2.4C

Tất cả các hoạt động cần phải thực hiện chính xác.

10.6.4.2.5 ASE_REQ.2.5C

Mỗi phụ thuộc của các yêu cầu an toàn cần không chỉ thỏa mãn mà sở cứ các yêu cầu an toàn cần biện minh cho các phụ thuộc mà không được thỏa mãn.

10.6.4.2.6 ASE_REQ.2.6C

Sở cứ các yêu cầu an toàn cần theo vết mỗi SFR trở lại các mục tiêu an toàn cho TOE.

10.6.4.2.7 ASE_REQ.2.7C

Sở cứ các yêu cầu an toàn cần chứng minh rằng SFR đáp ứng tất cả các mục tiêu an toàn cho TOE.

10.6.4.2.8 ASE_REQ.2.8C

Sở cứ các yêu cầu an toàn cần giải thích vì sao SAR được chọn.

10.6.4.2.9 ASE_REQ.2.9C

Tuyên bố các yêu cầu an toàn cần nhất quán nội bộ.

10.6.4.3 Các phần tử hành động của đánh giá viên

10.6.4.3.1 ASE_REQ.2.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

10.7 Đặc tả tổng quát TOE (ASE_TSS)

10.7.1 Mục tiêu

Đặc tả tổng quát TOE giúp đánh giá viên và khách hàng tiềm năng có được các hiểu biết chung về việc TOE được thực hiện như thế nào.

Đánh giá của đặc tả tổng quát TOE là cần thiết để quyết định mô tả TOE như thế nào là phù hợp:

- Đáp ứng các SFR của nó
- Bảo vệ chính nó chống lại sự can thiệp, sự giả mạo và phớt lờ ở mức logic.

Và các đặc tả tổng quát phải nhất quán với các mô tả hẹp khác của TOE.

10.7.2 Phân mức thành phần

Các thành phần trong họ này được phân mức dựa trên việc có hay không đặc tả tổng quát TOE là cần thiết để mô tả TOE đáp ứng SFR như thế nào, hay có hay không đặc tả tổng quát TOE cần thiết để mô tả làm thế nào TOE bảo vệ chính nó chống lại việc giả mạo hay phớt lờ ở mức logic. Sự mô tả bổ sung này có thể được sử dụng trong trường hợp đặc biệt tại nơi mà có thể liên quan xem xét kiến trúc an toàn TOE.

10.7.3 ASE_TSS.1 Đặc tả tổng quát TOE

Các phụ thuộc: ASE_INT.1 Giới thiệu ST

ASE_REQ.1 Tuyên bố các yêu cầu an toàn

ASE_REQ.1 Đặc tả chức năng cơ sở

10.7.3.1 Phần tử hành động của nhà phát triển

10.7.3.1.1 ASE_TSS.1.1D

Nhà phát triển cần cung cấp đặc tả tổng quát TOE

10.7.3.2 Các phần tử nội dung và trình bày

10.7.3.2.1 ASE_TSS.1.1C

Đặc tả tổng quát TOE cần mô tả TOE đáp ứng mỗi SFR như thế nào

10.7.3.3 Các phần tử hành động của đánh giá viên

10.7.3.3.1 ASE_TSS.1.1E

Đánh giá viên cần xác nhận rằng các thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày các chứng cứ

10.7.3.3.2 ASE_TSS.1.2E

Đánh giá viên cần xác nhận rằng đặc tả tổng quát TOE nhất quán với tổng quan TOE và mô tả TOE.

10.7.4 ASE_TSS.2 Đặc tả tổng quát với kiến trúc thiết kế tổng quát.

Các phụ thuộc: ASE_INT.1 Giới thiệu ST

ASE_REQ.1 Tuyên bố các yêu cầu an toàn

ASE_ARC.1 Mô tả các kiến trúc an toàn

10.7.4.1 Phần tử hành động của nhà phát triển

10.7.4.1.1 ASE_TSS.2.1D

Nhà phát triển cần cung cấp đặc tả tổng quát TOE

10.7.4.2 Các phần tử nội dung và trình bày

10.7.4.2.1 ASE_TSS.2.1C

Đặc tả tổng quát TOE cần mô tả TOE đáp ứng mỗi SFR như thế nào.

10.7.4.2.2 ASE_TSS.2.2C

Đặc tả tổng quát-TOE cần mô tả làm thế nào TOE tự bảo vệ chống lại sự can thiệp và sự giả mạo mức logic.

10.7.4.2.3 ASE_TSS.2.3C

Đặc tả tổng quát TOE cần mô tả TOE tự bảo vệ như thế nào để chống lại sự phớt lờ.

10.7.4.3 Các phần tử hành động của đánh giá viên

10.7.4.3.1 ASE_TSS.2.1E

Đánh giá viên cần xác nhận rằng các thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày các chứng cứ.

10.7.4.3.2 ASE_TSS.2.2E

Đánh giá viên cần xác nhận rằng đặc tả tổng quát TOE là nhất quán với tổng quan TOE và mô tả TOE.

11 Lớp ADV: Phát triển

Yêu cầu của lớp phát triển là cung cấp thông tin về TOE. Kiến thức có được từ thông tin này phải được sử dụng như là cơ sở để tạo ra bản phân tích điểm yếu và kiểm tra trên TOE như được mô tả trong lớp AVA và ATE.

Lớp phát triển bao gồm 6 họ các yêu cầu cho việc cấu trúc và biểu diễn TSF tại các mức thay đổi và các dạng thay đổi trừu tượng. Những họ này bao gồm:

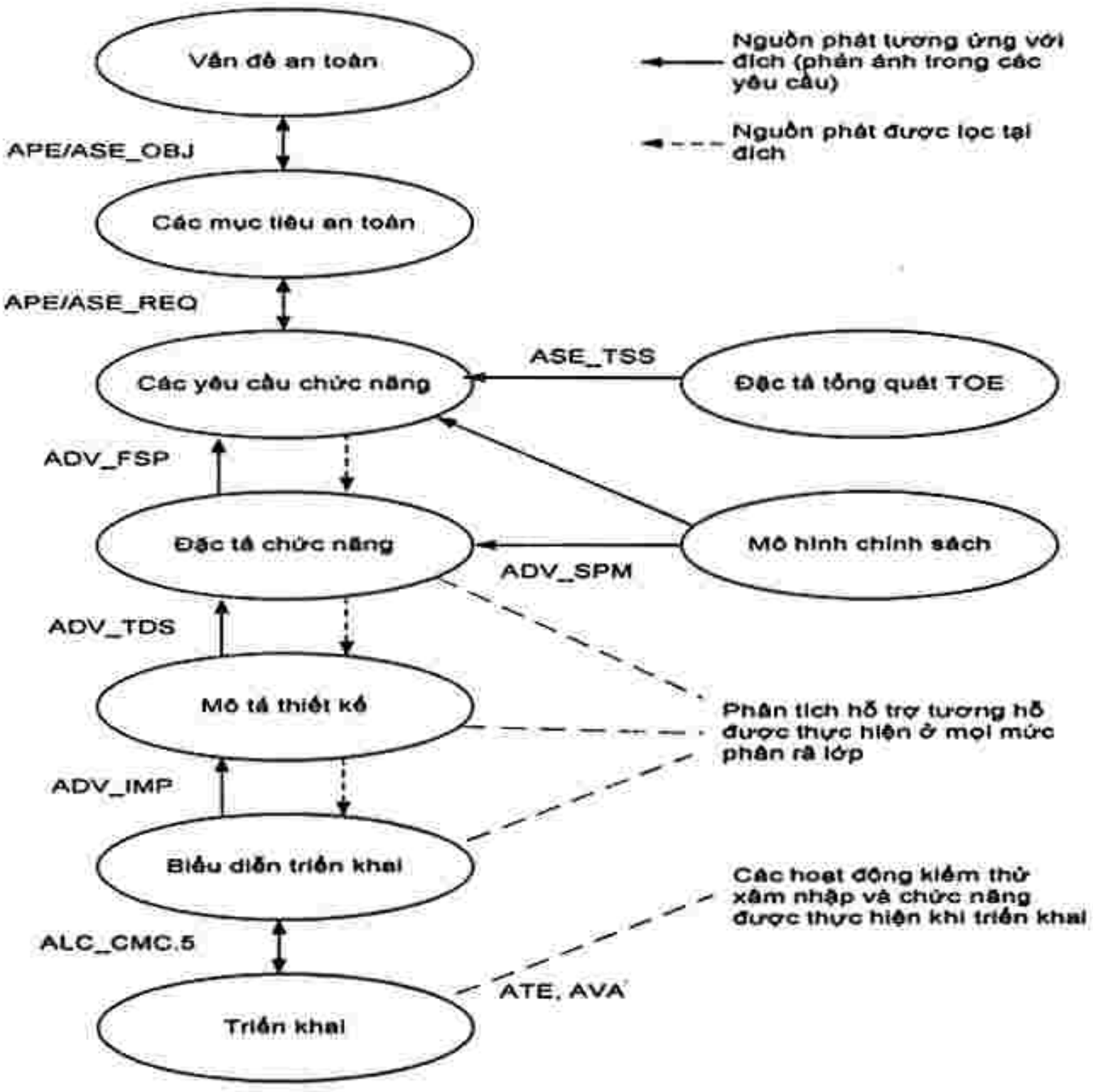
- Yêu cầu đối với mô tả thiết kế và thực hiện các SFR (ADV_FSP, ADV_TDS, ADV_IMP) (ở các mức độ trừu tượng khác nhau)
- Yêu cầu đối với mô tả về các tính năng hướng kiến trúc theo định hướng tách miền, khả năng tự bảo vệ và không thể vượt qua của TSF trong chức năng an toàn (ADV_ARC)
- Yêu cầu mô hình chính sách an toàn và cho ánh xạ tương ứng giữa các mô hình chính sách an toàn và đặc tả chức năng (ADV_SPM)
- Yêu cầu về cơ cấu nội bộ của TSF, bao gồm các khía cạnh như mô đun, phân lớp, và giảm thiểu độ phức tạp (ADV_INT).

Khi lập tài liệu các chức năng an toàn của TOE, có hai thuộc tính cần phải được chứng minh. Thuộc tính đầu tiên là các chức năng an toàn làm việc chính xác, có nghĩa là, nó thực hiện theo quy

định. Thuộc tính thứ hai, đòi hỏi một cách tiếp cận khó khăn hơn trong để chứng minh, theo đó TOE không thể được sử dụng theo cách như vậy mà các chức năng bảo mật có thể bị hỏng hoặc bỏ qua. Hai thuộc tính này yêu cầu một cách khác trong tiếp cận phân tích, và vì thế họ ADV được cấu trúc để hỗ trợ các phương pháp tiếp cận khác nhau. Các họ đặc tả chức năng (ADV_FSP), thiết kế TOE (ADV_TDS), biểu diễn triển khai (ADV_IMP), và mô hình chính sách an toàn (ADV_SPM) sẽ thực hiện với thuộc tính đầu tiên: đặc tả của chức năng an toàn. Các họ Kiến trúc (ADV_ARC) và TSF internals (ADV_INT) đối phó với các bất động sản thứ hai: các đặc điểm kỹ thuật của các thiết kế của TOE thể hiện các chức năng bảo mật không thể bị hỏng hoặc bỏ qua. Cần lưu ý rằng cả hai thuộc tính cần phải được nhận biết: thuộc tính càng bí mật được thỏa mãn thì TOE càng tin cậy. Các thành phần trong họ được thiết kế bởi vì sự đảm bảo tăng khi có được sự phân cấp tăng.

Các mô hình cho các họ nhắm mục tiêu vào các thuộc tính đầu tiên là một trong phân rã thiết kế. Ở mức cao nhất, có một đặc tả chức năng của TSF về giao diện của nó (mô tả những gì TSF làm để yêu cầu TSF cho các dịch vụ và trả lời kết quả), phân rã các TSF thành các đơn vị nhỏ hơn (Phụ thuộc vào việc bảo đảm mong muốn và sự phức tạp của TOE) và mô tả cách TSF đã thực hiện được chức năng của mình (với một mức độ chi tiết tương xứng với mức độ bảo đảm), và cho thấy việc thực hiện các TSF. Một mô hình chính thức của các hành vi an toàn cũng có thể được đưa ra. Tất cả các mức phân rã thường được sử dụng trong việc xác định tính đầy đủ và chính xác của các mức khác nhau, để đảm bảo rằng các mức có hỗ trợ lẫn nhau. Các yêu cầu để biểu diễn TSF khác nhau được tách thành các họ khác nhau, để cho phép các tác giả PP / ST chỉ ra các biểu diễn TSF nào được yêu cầu. Mức độ được lựa chọn sẽ quyết định dự đoán bảo đảm hay mong muốn sẽ đạt được.

Hình 10 chỉ ra các mối quan hệ giữa sự biểu diễn TSF khác nhau của lớp ADV, cũng như mối quan hệ của chúng với các lớp khác. Số liệu cho thấy, các lớp APE và ASE định nghĩa các yêu cầu về sự tương ứng giữa các SFR và các mục tiêu an toàn cho TOE. Lớp ASE cũng định nghĩa các yêu cầu cho sự tương ứng giữa hai mục tiêu an toàn và SFR, và với các đặc tả tóm tắt TOE để giải thích làm thế nào TOE đáp ứng SFR của nó. Các hoạt động của ALC_CMC.5.2E bao gồm việc xác minh rằng các TSF đã được kiểm thử với lớp ATE và AVA trong thực tế, một trong những mô tả của tất cả các cấp mức độ phân rã ADV.



Hình 10 - Mối quan hệ của các cấu trúc ADV với lớp khác và các họ khác

Các yêu cầu cho tất cả các đáp ứng khác thể hiện trong hình 10 được định nghĩa trong lớp ADV. Các mô hình chính sách an toàn họ (ADV_SPM) xác định các yêu cầu về mô hình chính thức SFR được chọn, và cung cấp đáp ứng giữa các đặc tả chức năng và mô hình chính thức. Mỗi họ đảm bảo cụ thể cho một đại diện TSF (tức là chức năng đặc điểm kỹ thuật (ADV_FSP), thiết kế TOE (ADV_TDS) và biểu diễn triển khai (ADV_IMP)) xác định các yêu cầu liên quan mà TSF đại diện cho các SFR. Tất cả các phân rã phải phản ánh chính xác tất cả các phân rã khác (ví dụ, có thể hỗ trợ lẫn nhau); Nhà phát triển cung cấp khả năng theo vết với phần tử C cuối của các thành phần. Bảo đảm liên quan đến yếu tố này là thu được trong quá trình phân tích cho từng mức độ phân rã bằng cách tham chiếu đến mức độ khác của sự phân rã (một cách đệ quy) trong khi các phân tích của một mức độ cụ thể của việc phân rã đang được thực hiện; Đánh giá viên thẩm tra sự tương ứng như là một phần của phần tử E thứ hai. Những hiểu biết thu được từ các mức độ phân rã tạo thành cơ sở của những nỗ lực kiểm thử chức năng và thâm nhập.

Họ ADV_INT không được biểu diễn trong hình này, vì nó có liên quan đến cấu trúc bên trong của TSF, và liên quan gián tiếp đến quá trình tinh chỉnh các đại diện của TSF. Tương tự, họ ADV_ARC là không được biểu diễn trong hình vì nó liên quan đến tính hợp lý kiến trúc, hơn là việc biểu diễn, của các TSF. Cả ADV_INT và ADV_ARC liên quan đến việc phân tích các thuộc tính mà các TOE không thể thực hiện để phá vỡ hoặc làm hỏng chức năng an toàn của nó.

Chức năng an toàn TOE (TSF) bao gồm tất cả các phần của TOE mà cần phải dựa vào thực thi của SFR. TSF bao gồm cả chức năng trực tiếp thực thi các SFR, cũng như các chức năng đó, mà không trực tiếp thực thi các SFR, góp phần thực thi của chúng một cách gián tiếp nhiều hơn, bao gồm cả chức năng với khả năng là nguyên nhân các SFR bị vi phạm. Điều này bao gồm các phần của TOE được viện dẫn lúc bắt đầu mà có trách nhiệm đưa TSF vào trạng thái an toàn ban đầu của nó.

Một số khái niệm quan trọng được sử dụng trong sự phát triển của các thành phần của họ ADV. Những khái niệm, được giới thiệu ngắn gọn ở đây, được giải thích đầy đủ hơn trong các ghi chú cho các họ.

Một quan điểm chỉ ra là càng nhiều thông tin sẵn sàng thì càng đạt được mức độ đảm bảo cao hơn về chức năng an toàn thông tin. 1) được thực hiện chính xác, 2) không thể bị sửa đổi và 3) không thể bị vượt qua. Điều này được thực hiện thông qua việc thẩm tra sự nhất quán và chính xác của các tài liệu với các tài liệu khác, và với việc cung cấp thông tin có thể được sử dụng để đảm bảo rằng các hoạt động kiểm tra là toàn diện (cả hai kiểm tra về chức năng và thâm nhập). Điều này được phản ánh sự phân mức thành phần của họ. Nhìn chung, các thành phần được phân mức dựa trên số lượng thông tin mà được cung cấp (và được phân tích sau đó).

Mặc dù không phải đúng với tất cả các TOE, trong trường hợp nói chung khi TSF có đủ phức tạp mà có các phần của TSF được kiểm tra tăng cường hơn các phần khác của TSF. Không may việc quyết định các phần này có phần chủ quan, do đó thuật ngữ và thành phần đã được định nghĩa như vậy mà là mức tăng đảm bảo, trách nhiệm trong việc quyết định các phần nào của TSF cần phải xem xét thay đổi chi tiết từ nhà phát triển đến đánh giá viên. Để hỗ trợ trong việc thể hiện khái niệm này, theo các thuật ngữ được giới thiệu. Cần lưu ý rằng trong các họ của lớp, thuật ngữ này được sử dụng khi biểu diễn các phần liên quan đến SFR của TOE (nghĩa là, các phần tử và các đơn vị làm việc thể hiện bên trong các đặc tả chức năng (ADV_FSP), thiết kế TOE (ADV_TDS), và biểu diễn thực hiện của các họ (ADV_IMP)). Khi đó, khái niệm chung (với một số phần của TOE hấp dẫn hơn các phần khác) được áp dụng với các họ khác, tiêu chi này được biểu diễn dưới cách khác để đạt được yêu cầu đảm bảo.

Tất cả các phần của TSF là phù hợp an toàn, nghĩa là chúng cần phải bảo vệ an toàn của TOE như được biểu diễn bởi các SFR và các yêu cầu cho việc chia cắt miền và không thể đi đường vòng. Một khía cạnh phù hợp an toàn khác là mức độ mà một phần của TSF thực thi yêu cầu an toàn. Các phần khác nhau của TOE thực hiện các vai trò khác nhau (hoặc vai trò không rõ ràng ở tất cả) trong việc thực thi các yêu cầu an toàn, điều này tạo ra một sự liên tục với SFR liên quan: tại một đầu của sự liên tục này là các phần của TOE được gọi là thực thi-SFR. Các phần này đóng một vai trò trực tiếp trong việc thực hiện bất kỳ SFR nào trong TOE này. SFR như thế tham chiếu đến bất kỳ chức năng cung cấp bởi một trong những SFR có trong ST này. Cần lưu ý rằng việc định nghĩa của việc thực hiện vai trò trong chức năng thực thi-SFR là không thể biểu diễn số lượng. Ví dụ, trong việc thực hiện cơ chế kiểm soát truy nhập tùy ý (DAC), cái nhìn hẹp thực thi-SFR có thể chỉ là một vài dòng mã thực sự thực hiện việc kiểm tra các thuộc tính của chủ thể chống lại các thuộc tính của đối tượng. Một cái nhìn rộng hơn sẽ bao gồm các thực thể phần mềm (ví dụ, chức năng C) có chứa một số dòng mã. Một cái nhìn rộng hơn vẫn sẽ bao gồm những người gọi của chức năng C, bởi vì chúng sẽ chịu trách nhiệm thi hành quyết định được trả về bởi việc kiểm tra thuộc tính. Một cái nhìn rộng hơn sẽ bao gồm bất kỳ mã nào trong cây gọi (hoặc chương trình tương đương cho việc thực hiện các ngôn ngữ được sử dụng) cho chức năng C đó (ví dụ, một chức năng sắp xếp mà các thực thể trong danh sách điều khiển truy cập được sắp xếp sử dụng thuật toán first-match – chọn phù hợp đầu tiên). Tại một số điểm, thành phần này không được thực thi nhiều trong sách an toàn, mà đóng vai trò hỗ trợ, các thành phần như vậy được gọi là hỗ trợ SFR.

Một trong các tính chất của chức năng hỗ trợ SFR là nó được tin cậy để thực hiện việc chỉnh sửa việc thực hiện SFR trong qua trình áp dụng mà không có lỗi. Chức năng này có thể bị phụ thuộc vào chức năng thực thi SFR, nhưng các mối phụ thuộc này thường ở mức độ chức năng, ví dụ như quản lý bộ nhớ, quản lý bộ đệm, v.v... Việc giảm liên tục độ tương quan an toàn được gọi là không can thiệp vào SFR (SFR no-interfering). Chức năng như vậy không có vai trò trong việc thực hiện các SFR, và là một phần tương tự của TSF vì môi trường của nó: ví dụ, bất kỳ mã chạy trong một chế độ phần cứng đặc quyền của hệ điều hành. Nó cần phải được coi là một phần của TSF bởi vì, nếu bị xâm nhập (hoặc

thay thế bởi mã độc hại), nó có thể làm ảnh hưởng tới hoạt động chính xác của SFR bởi ưu điểm của việc hoạt động trong chế độ phần cứng đặc quyền. Một ví dụ về chức năng không can thiệp vào SFR có thể là một tập hợp các ứng dụng dấu chấm động trong toán học nổi thực hiện chế độ nhân cho các suy xét về tốc độ.

Họ kiến trúc (Kiến trúc an toàn (ADV_ARC)) cung cấp các yêu cầu và phân tích của TOE dựa trên các thuộc tính phân tách miền, tự bảo vệ, và không thể vượt qua. Những thuộc tính liên quan đến các SFR trong đó, nếu những thuộc tính này không có mặt, nó có thể sẽ dẫn đến lỗi của các cơ chế thực hiện SFR. Chức năng và thiết kế liên quan đến các thuộc tính này không được coi là một phần trong mô tả liên tục ở trên, nhưng thay vì được xử lý riêng do bản chất khác nhau của nó và các yêu cầu phân tích.

Sự khác biệt trong phân tích việc thực hiện các SFR (chức năng thực thi SFR và hỗ trợ SFR) và thực hiện một số thuộc tính an toàn nền tảng khác của TOE, bao gồm các vấn đề liên quan khởi tạo, tự bảo vệ và không thể vượt qua, đó là chức năng liên quan đến SFR mà nhiều hay ít có thể thấy được trực tiếp và tương đối dễ dàng cho việc kiểm tra, khi đó các thuộc tính được đề cập ở trên yêu cầu các mức độ phân tích khác nhau trong các tập rộng hơn nhiều của chức năng. Hơn nữa, độ sâu phân tích các thuộc tính đó sẽ thay đổi phụ thuộc vào thiết kế của TOE. Họ ADV được xây dựng để giải quyết điều này bằng một họ riêng biệt (Kiến trúc an toàn (ADV_ARC)) dành cho việc phân tích các yêu cầu khởi tạo, tự bảo vệ, và không thể vượt qua, trong khi các họ khác có liên quan với phân tích các chức năng hỗ trợ SFR.

Ngay cả trong trường hợp các mô tả khác nhau là cần thiết cho nhiều cấp độ trừu tượng, nó không phải là hoàn toàn cần thiết cho mỗi và mọi đại diện TSF chứa trong một văn bản riêng. Thật vậy, nó có thể là trường hợp mà một tài liệu duy nhất đáp ứng các yêu cầu lập tài liệu cho việc biểu diễn nhiều hơn một TSF, vì nó là thông tin về mỗi cái trong các đại diện TSF đó là cần thiết, hơn là các cấu trúc tài liệu kết quả. Trong trường hợp nhiều đại diện TSF được kết hợp trong một tài liệu duy nhất, các nhà phát triển nên chỉ ra các phần của tài liệu đáp ứng được yêu cầu.

Ba loại kiểu đặc tả kỹ thuật được uỷ quyền của lớp này: không chính thức, bán chính thức và chính thức. Các đặc tả chức năng và tài liệu thiết kế TOE luôn luôn được viết bằng một trong hai phong cách chính thức hoặc bán chính thức. Kiểu bán chính thức làm giảm sự không rõ ràng trong các tài liệu này trên một bài trình bày không chính thức. Một đặc tả chính thức có thể được yêu cầu thêm vào các bài trình bày bán chính thức, giá trị này là một mô tả của TSF trong nhiều hơn một cách sẽ tăng thêm bảo đảm rằng các TSF đã được xác định hoàn toàn và chính xác.

Một đặc điểm kỹ thuật không chính thức được viết dưới dạng văn xuôi trong ngôn ngữ thông dụng. Ngôn ngữ được sử dụng ở đây là ý nghĩa truyền thông trong bất kỳ tiếng nói chung (ví dụ như tiếng Tây Ban Nha, tiếng Đức, tiếng Pháp, tiếng Anh, tiếng Hà Lan). Một đặc tả kỹ thuật không chính thức không phải là chủ thể của bất kỳ ký hiệu hoặc sự hạn chế đặc biệt nào khác so với những yêu cầu như quy ước thông thường cho ngôn ngữ đó (ví dụ văn phạm và cú pháp). Trong khi không áp dụng hạn chế các chú giải, các đặc tả không chính thức cũng được yêu cầu để cung cấp các định nghĩa có ý nghĩa cho các thuật ngữ được sử dụng trong một ngữ cảnh khác hơn là chấp nhận sử dụng thông thường.

Sự khác biệt giữa tài liệu bán chính thức và chính thức chỉ là vấn đề định dạng hay trình bày: một ký hiệu bán chính thức bao gồm những thứ như một ký hiệu rõ ràng, một định dạng trình bày tiêu chuẩn hóa, v.v... Một đặc tả bán chính thức được viết theo mẫu trình bày tiêu chuẩn. Các bài trình bày nên sử dụng các thuật ngữ nhất quán khi viết bằng một ngôn ngữ thông dụng. Bài trình bày cũng có thể sử dụng ngôn ngữ nhiều cấu trúc/biểu đồ hơn (ví dụ như sơ đồ lưu lượng dữ liệu, biểu đồ chuyển trạng thái, sơ đồ mối quan hệ các thực thể, sơ đồ cấu trúc dữ liệu, và sơ đồ tiến trình hay sơ đồ cấu trúc chương trình). Cho dù có dựa trên sơ đồ hoặc ngôn ngữ thông dụng, một tập hợp các quy ước phải

được sử dụng khi trình bày. Thuật ngữ này xác định một cách rõ ràng các từ đang được sử dụng một cách chính xác và không thay đổi; tương tự, định dạng chuẩn nói lên việc quan tâm đặc biệt được thực hiện công tác chuẩn bị tài liệu một cách rõ ràng nhất. Nó nên được lưu ý rằng phần cơ bản khác nhau của TSF có thể có các quy ước và kiểu biểu diễn ký hiệu bán hình thức khác nhau (miễn là số lượng "ký hiệu bán hình thức" khác nhau là nhỏ), điều này vẫn tuân thủ các khái niệm về trình bày bán hình thức.

Một đặc tả chính thức được viết dưới dạng ký hiệu dựa trên các khái niệm toán học được xây dựng tốt, và thường đi kèm với hỗ trợ giải thích (chính thức) dưới dạng văn xuôi. Những khái niệm toán học được sử dụng để định nghĩa cú pháp và ngữ nghĩa của các ký hiệu và các quy tắc chứng minh có hỗ trợ nguyên nhân về mặt logic. Các quy tắc cú pháp và ngữ nghĩa hỗ trợ một ký hiệu chính thức mà định nghĩa làm thế nào để nhận biết các cấu trúc rõ ràng và xác định ý nghĩa của chúng. Cần có bằng chứng rằng không thể là nguồn gốc mâu thuẫn, và tất cả các quy tắc hỗ trợ các ký hiệu cần phải được xác định hoặc tham chiếu.

Hình 11 cho thấy các Họ bên trong lớp này, và phân cấp của các thành phần bên trong họ.

Hình 11 – Phân cấp lớp ADV: Phát triển

11.1 Kiến trúc an toàn (ADV_ARC)

11.1.1 Mục tiêu

Các mục tiêu của họ này là phục vụ nhà phát triển để cung cấp khả năng mô tả kiến trúc an toàn của TSF. Điều này sẽ cho phép phân tích thông tin, khi kết hợp với các chứng cứ khác để biểu diễn cho các TSF, để xác nhận TSF các đạt được các thuộc tính mong muốn. Mô tả kiến trúc an toàn hỗ trợ giải thích các yêu cầu ngầm hiểu về phân tích an toàn của TOE có thể đạt được bằng cách kiểm tra các TSF, mà không có một kiến trúc rõ ràng, toàn bộ các chức năng TOE cần phải được kiểm tra.

11.1.2 Phân mức thành phần

Họ này chỉ chứa một thành phần.

11.1.3 Chú thích ứng dụng

Các thuộc tính tự bảo vệ, tách miền, và không thể vượt qua được phân biệt với chức năng an toàn thể hiện bằng Phần 2 SFR vì tự bảo vệ và không thể vượt qua phần lớn không có giao diện trực tiếp quan sát tại các TSF. Thay vào đó, chúng là thuộc tính của TSF được đạt được thông qua thiết kế của TOE và TSF, và được thực thi bởi việc thực hiện chính xác thiết kế đó.

Cách tiếp cận sử dụng họ này là dành cho nhà phát triển để thiết kế và cung cấp TSF trình bày các thuộc tính nêu trên, và để cung cấp bằng chứng (dưới dạng tài liệu) để giải thích các thuộc tính của TSF. Việc giải thích này cung cấp mức độ cụ thể như mô tả các phần tử thực thi SFR của TOE trong tài liệu thiết kế TOE. Đánh giá viên có trách nhiệm xem xét chứng cứ và, cùng với các bằng chứng khác của TOE và TSF, quyết định các thuộc tính này sẽ đạt được.

Đặc tả của thực hiện chức năng an toàn cho các SFR (trong đặc tả chức năng (ADV_FSP) và thiết kế TOE (ADV_TDS) sẽ không cần thiết có các cơ chế mô tả được sử dụng trong việc thực hiện cơ chế tự bảo vệ và không thể vượt qua (ví dụ cơ chế quản lý bộ nhớ). Do đó, cần thiết cung cấp sự đảm bảo rằng các yêu cầu được đạt được là phù hợp hơn để biểu diễn phân tách giữa sự phân rã thành phần thiết kế của TSF như thể hiện trong ADV_FSP và ADV_TDS. Điều này không có hàm ý rằng mô tả kiến trúc an toàn được gọi bởi thành phần này có thể không tham khảo hoặc sử dụng phân rã thiết kế, nhưng dường như có rất nhiều chi tiết hiện tại trong tài liệu phân rã sẽ không có liên quan đến các đối số được cung cấp cho tài liệu mô tả kiến trúc an toàn.

Mô tả kiến trúc hợp lý có thể được dùng như phân tích tính dễ tổn thương của nhà phát triển, trong đó nó cung cấp sự biện minh cho lý do tại sao TSF là hợp lý và thực thi tất cả các SFR của nó. Tính hợp lý đạt được tại thông qua cơ chế an toàn cụ thể, chúng sẽ được kiểm tra như một phần của yêu cầu độ sâu (ATE_DPT), tại nơi tính hợp lý đạt được chỉ duy nhất thông qua kiến trúc, hành vi đó sẽ được kiểm thử như là một phần của AVA: yêu cầu đánh giá tính dễ tổn thương.

Họ này bao gồm các yêu cầu cho mô tả kiến trúc an toàn mà mô tả tính chất tự bảo vệ, tách miền, không thể vượt qua, bao gồm một mô tả về việc làm thế nào mà các tính chất này được hỗ trợ bởi các phần của TOE mà được sử dụng cho khởi tạo TSF.

Thông tin bổ xung về các thuộc tính kiến trúc an toàn về tự bảo vệ, tách miền, và không thể vượt qua có thể được tìm thấy trong Phụ lục A.1, ADV_ARC: bổ sung tài liệu về kiến trúc an toàn.

11.1.4 ADV_ARC.1 Mô tả kiến trúc an toàn

Các phụ thuộc: ADV_FSP.1 Đặc tả chức năng cơ sơ

ADV_TDS.1 Thiết kế cơ sơ

11.1.4.1 Phần tử hành động của nhà phát triển

11.1.4.1.1 ADV_ARC.1.1D

Nhà phát triển cần thiết kế và thực hiện TOE mà các đặc trưng an toàn của TSF không thể bị vượt qua.

11.1.4.1.2 ADV_ARC.1.2D

Nhà phát triển cần thiết kế và thực hiện TSF mà có thể bảo vệ chính nó bởi sự pha trộn của các thực thể không tin cậy.

11.1.4.1.3 ADV_ARC.1.3D

Nhà phát triển cần cung cấp mô tả kiến trúc an toàn của TSF.

11.1.4.2 Các phần tử nội dung và trình bày

11.1.4.2.1 ADV_ARC.1.1C

Mô tả kiến trúc an toàn cần thực hiện tại mức độ chi tiết bằng với mô tả tóm tắt thực thi SFR trong tài liệu thiết kế TOE.

11.1.4.2.2 ADV_ARC.1.2C

Mô tả kiến trúc an toàn cần mô tả việc bảo trì các miền an toàn với sự nhất quán của TSF so với SFR.

11.1.4.2.3 ADV_ARC.1.3C

Mô tả kiến trúc an toàn cần mô tả làm thế nào tiến trình khởi tạo TSF là an toàn.

11.1.4.2.4 ADV_ARC.1.4C

Mô tả kiến trúc an toàn cần chứng minh rằng TSF bảo vệ chính nó khỏi bị can thiệp.

11.1.4.2.5 ADV_ARC.1.5C

Mô tả kiến trúc an toàn cần chứng minh rằng TSF chống lại việc vượt qua của chức năng thực thi SFR.

11.1.4.3 Phần tử hành động của đánh giá viên

11.1.4.3.1 ADV_ARC.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và biểu diễn các chứng cứ.

11.2 Đặc tả chức năng (ADV_FSP)

11.2.1 Mục tiêu

Các yêu cầu họ dựa trên các đặc tả chức năng, trong đó mô tả các giao diện TSF (TSFI). Các TSFI bao gồm tất cả các phương tiện cho người dùng để gọi một dịch vụ từ TSF (bằng cách cung cấp dữ liệu được xử lý bởi TSF) và các câu trả lời tương ứng với những lệnh gọi dịch vụ. Nó không mô tả cách các tiến trình TSF yêu cầu các dịch vụ, cũng không mô tả cách thức truyền thông khi TSF các gọi dịch vụ từ môi trường áp dụng của nó; thông tin này được đề cập thông qua việc thiết kế TOE (ADV_TDS) và sự tin cậy của các thành phần phụ thuộc của họ (ACO_REL) tương ứng.

Họ này cung cấp đảm bảo trực tiếp bằng cách cho phép đánh giá viên hiểu cách TSF đáp ứng các SFR đã tuyên bố. Nó cũng cung cấp bảo đảm gián tiếp, như là đầu vào cho các họ và lớp đảm bảo:

- ADV_ARC, nơi mà sự mô tả của các TSFI có thể được sử dụng để đạt được sự hiểu biết tốt hơn về cách TSF được bảo vệ chống lại sự phá hủy (như tự bảo vệ chống lại sự phá hoại hay tách miền) và/hoặc bỏ qua;
- ATE, nơi mà sự mô tả của các TSFI là một đầu vào quan trọng cho cả nhà phát triển và đánh giá viên kiểm thử;
- AVA, là nơi việc mô tả của các TSFI được sử dụng để tìm kiếm các điểm yếu.

11.2.2 Phân mức thành phần

Các thành phần trong họ này được phân mức dựa trên mức độ yêu cầu chi tiết của việc mô tả TSFI, và mức độ yêu cầu về hình thức việc mô tả các TSFI.

11.2.3 Chú thích ứng dụng

Một khi các TSFI được xác định (xem A.2.1, Xác định TSFI để được hướng dẫn và ví dụ về xác định TSFI), chúng đã được mô tả. Tại các thành phần mức thấp hơn, nhà phát triển tập trung vào các tài liệu của họ (và đánh giá viên tập trung vào các phân tích của họ) trên nhiều khía cạnh an toàn liên

quan của TOE. Ba loại TSFI được xác định, dựa trên quan hệ của các dịch vụ có sẵn thông qua đó chúng để có các SFR được tuyên bố:

- Nếu một dịch vụ có sẵn thông qua một giao diện có thể được truy nguồn từ một trong những SFR áp cho TSF, khi đó giao diện được gọi là thực thi-SFR. Lưu ý rằng có thể xảy ra trường hợp một giao diện có thể có nhiều loại dịch vụ và kết quả, một số trong đó có thể thực thi SFR và một số khác có thể không.
- Giao diện (hoặc dịch vụ có sẵn thông qua một giao diện liên quan) cho các dịch vụ mà chức năng thực thi SFR được dựa trên đó, nhưng chỉ cần thực hiện chức năng chính xác để cho các chính sách an toàn của TOE được bảo vệ, được gọi là hỗ trợ SFR.
- Giao diện với các dịch vụ trên đó chức năng thực thi SFR không có các mối phụ thuộc được gọi là không can thiệp vào SFR.

Cần lưu ý rằng để cho một giao diện được hỗ trợ SFR hay không can thiệp SFR thì nó phải không có các kết quả hay dịch vụ thực thi SFR. Ngược lại, giao diện thực thi SFR có thể có các dịch vụ hỗ trợ SFR (Ví dụ như khả năng thiết lập đồng hồ hệ thống có thể là một dịch vụ thực thi SFR của giao diện, nhưng nếu cùng một giao diện được sử dụng để hiển thị ngày hệ thống dịch vụ có thể hỗ trợ SFR). Một ví dụ về một giao diện hoàn toàn hỗ trợ SFR là một giao diện cuộc gọi hệ thống được sử dụng cả bởi người dùng và do một phần của TSF nghĩa là đang hoạt động dựa trên hành vi của người dùng.

Khi có thêm thông tin về các TSFI, mức độ lớn hơn của đảm bảo có thể đạt được với giao diện được phân loại / phân tích chính xác. Các yêu cầu được cấu trúc như vậy, ở mức thấp nhất, các thông tin cần thiết cho giao diện không can thiệp SFR là tối thiểu cần thiết để đánh giá viên quyết định theo một cách hiệu quả. Ở cấp độ cao hơn, nếu có thêm thông tin đánh giá viên sẽ có thêm sự tin cậy trong các thiết kế.

Mục đích trong việc xác định các nhãn này (Thực thi, hỗ trợ, không can thiệp với SFR) và đưa ra các yêu cầu khác nhau theo từng cái (ở các thành phần đảm bảo mức thấp hơn) để cung cấp một phép xấp xỉ bước đầu của nơi tập trung phân tích và bằng chứng mà phân tích được thực hiện dựa trên nó. Nếu các tài liệu của nhà phát triển của các giao diện TSF mô tả tất cả các giao diện theo mức quy định trong các yêu cầu đối với các giao diện thực thi SFR (có nghĩa là, nếu lập tài liệu vượt quá yêu cầu), không cần thiết phải cho phát triển tạo ra các bằng chứng mới phù hợp với yêu cầu. Tương tự như vậy, bởi vì các nhãn chỉ đơn thuần là một phương tiện phân biệt các loại giao diện trong các yêu cầu, nó không cần cho các nhà phát triển khi cập nhật các bằng chứng duy nhất để gán cho các giao diện như thực thi-SFR, hỗ trợ SFR, không can thiệp SFR. Mục đích chính của nhãn này là cho phép nhà phát triển có ít kiến thức để phát triển phương pháp luận (và hiện vật, chẳng hạn như giao diện chi tiết và tài liệu thiết kế) để cung cấp bằng chứng cần thiết chỉ mà không phải chi phí quá mức.

Các phần tử C cuối cùng của mỗi thành phần trong họ này cung cấp một sự tương ứng trực tiếp giữa các SFR và đặc tả chức năng, đó là một dấu hiệu trong đó có giao diện được sử dụng để gọi đến từng tuyên bố SFR. Trong trường hợp ST có chứa các yêu cầu chức năng như: Bảo vệ thông tin còn sót lại (FDP_RIP) - TCVN 8709-2, mà có chức năng có thể không biểu hiện chính mình trong TSFIs, các đặc tả chức năng và/hoặc các truy gốc được chờ đợi sẽ xác định các SFR này, bao gồm chúng trong các đặc tả chức năng giúp đảm bảo rằng chúng không bị mất ở mức thấp hơn của phân rã, nơi chúng có liên quan.

11.2.3.1 Chi tiết về các giao diện

Các yêu cầu định nghĩa các bộ sưu tập của các chi tiết về TSFI là được cung cấp. Với mục đích của các yêu cầu, giao diện được chỉ ra (trong mức độ chi tiết khác nhau) về mục tiêu của chúng, phương pháp sử dụng, thông số, mô tả thông số, và thông báo lỗi.

Mục đích của giao diện là một mô tả mức cao các mục tiêu chung của giao diện (ví dụ các lệnh tiến trình GUI, tiếp nhận các gói tin mạng, cung cấp đầu ra máy in v.v...).

Phương pháp sử dụng của giao diện mô tả việc làm thế nào giao diện được hỗ trợ để sử dụng. Mô tả này nên được xây dựng xung quanh các tương tác khác nhau hiện có tại giao diện đó. Ví dụ, nếu giao diện là một dấu nhắc lệnh Unix, ls, mv và cp có thể tương tác với giao diện đó. Đối với mỗi tương tác phương pháp sử dụng mô tả những gì tương tác này thực hiện, cả hành vi nhìn thấy ở giao diện (ví dụ như chương trình gọi các API, người dùng Windows thay đổi một thiết lập trong thanh ghi v.v...) cũng như hành vi tại các giao diện khác (ví dụ như tạo ra một bản ghi phục vụ kiểm tra).

Tham số được đầu vào và đầu ra rõ ràng từ một giao diện điều khiển hành vi của giao diện đó. Ví dụ, các thông số là các đối số cung cấp cho một API; các lĩnh vực khác nhau trong một gói tin cho một giao thức mạng nhất định; các giá trị khóa riêng trong thanh ghi của Windows, các tín hiệu trên một tập hợp các chân trên một con chip, những cờ có thể được thiết lập cho lệnh ls v.v.... Các tham số được "nhận diện" với một danh sách đơn giản của những gì chúng đang có.

Mô tả tham số nói lên rằng tham số này có ý nghĩa gì. Ví dụ, một mô tả tham số chấp nhận được đối với giao diện foo (i) sẽ là "tham số i là một số nguyên cho biết số lượng người dùng hiện đang đăng nhập vào hệ thống". Một mô tả như là "tham số i là một số nguyên" là không thể chấp nhận được.

Mô tả các hành động của một giao diện mô tả những gì mà giao diện thực hiện. Điều này là chi tiết hơn mục đích trong đó, trong khi các "mục đích" giải thích lý do tại sao người ta muốn sử dụng nó, còn "hành động" cho thấy tất cả mọi thứ mà nó làm. Những hành động này có thể liên quan hoặc không liên quan đến các SFR. Trong trường hợp hành động của giao diện không có liên quan đến SFR, mô tả của nó được nói tóm tắt, có nghĩa là mô tả chỉ nêu rõ rằng nó thực sự là không liên quan đến SFR.

Các mô tả thông báo lỗi xác định các điều kiện tạo ra nó, thông điệp là gì, và ý nghĩa của bất kỳ mã lỗi nào. Một thông báo lỗi được tạo ra bởi các TSF để chỉ ra rằng một vấn đề hoặc sự bất thường ở một mức độ nào đó đã thu được. Các yêu cầu trong họ này đề cập đến các loại thông báo lỗi khác nhau:

- Một thông báo lỗi "trực tiếp" là một phản ứng an toàn có liên quan thông qua lệnh gọi TSFI cụ thể.
- Lỗi "gián tiếp" có thể không được gắn với một lời gọi TSFI cụ thể bởi vì nó là kết quả của điều kiện toàn hệ thống (ví dụ như cạn kiệt tài nguyên, gián đoạn kết nối, v.v...) Thông báo lỗi mà không liên quan bảo mật cũng được xem là "gián tiếp".
- Lỗi "còn lại" là bất kỳ lỗi nào khác, chẳng hạn như những cái mà có thể được tham chiếu trong mã. Ví dụ, việc sử dụng đoạn mã kiểm tra điều kiện để kiểm tra các điều kiện mà xuất hiện không hợp lý (ví dụ như một kết thúc "else" sau khi một danh sách các "case"), sẽ cung cấp để tạo ra thông điệp bắt lỗi, trong TOE sử dụng, các thông báo lỗi này sẽ không bao giờ được nhìn thấy.

Một ví dụ về đặc tả chức năng được cung cấp trong A.2.3.

11.2.3.2 Các thành phần của họ này

Tăng cường bảo đảm thông qua sự tăng hoàn thiện và độ chính xác trong đặc tả giao diện được phản ánh trong các tài liệu cần thiết từ nhà phát triển như chi tiết trong các thành phần phân cấp trong họ này.

Trong đặc tả chức năng cơ bản ADV_FSP.1, chỉ các tài liệu hướng dẫn được yêu cầu có tính chất của tất cả các TSFIs và mô tả ở mức cao của TSFI thực thi SFR và hỗ trợ SFR. Để cung cấp thêm một vài đảm bảo, mà các khía cạnh "quan trọng" của TSF có tính chất chính xác tại các TSFI, nhà phát triển

được yêu cầu cung cấp mục đích và phương pháp sử dụng, các tham số cho thực thi SFR và hỗ trợ SFR của TSFIs.

Tại đặc tả chức năng thực thi an toàn ADV_FSP.2, nhà phát triển được yêu cầu cung cấp các mục đích, phương pháp sử dụng, thông số, và mô tả thông số cho tất cả TSFIs. Thêm vào đó, đối với TSFI thực thi SFR, nhà phát triển cần phải mô tả các hành động thực thi SFR và các thông báo lỗi trực tiếp.

Theo đặc tả chức năng với bản tóm tắt hoàn chỉnh ADV_FSP.3, nhà phát triển phải cung cấp ngay, ngoài các thông tin cần thiết tại ADV_FSP.2, cung cấp đủ thông tin về hỗ trợ SFR và không can thiệp SFR để chứng minh rằng chúng không phải là thực thi SFR. Thêm vào đó, nhà phát triển phải lập tài liệu tất cả các thông báo lỗi trực tiếp do việc gọi các TSFI của thực thi SFR.

Theo đặc tả chức năng đầy đủ ADV_FSP.4, tất cả các TSFI - cho dù thực thi SFR, hỗ trợ SFR, không can thiệp SFR - phải được mô tả ở cùng mức độ như nhau, bao gồm tất cả các thông báo lỗi trực tiếp.

Theo đặc tả chức năng bán chính thức đầy đủ với các thông tin lỗi bổ sung ADV_FSP.5, mô tả TSFI cũng bao gồm các thông báo lỗi mà không phải là kết quả của việc gọi của TSFI.

Theo ADV_FSP.6 đặc tả chức năng bán chính thức đầy đủ với bổ sung đặc tả chính thức, ngoài các thông tin theo yêu cầu của ADV_FSP.5, tất cả các thông báo lỗi còn lại đã được bao gồm. Nhà phát triển cũng phải cung cấp mô tả chính thức của TSFI. Điều này cung cấp một cái nhìn khác của TSFI có thể phơi bày các đặc tả không nhất quán hay không hoàn tất.

11.2.4 ADV_FSP.1 Đặc tả chức năng cơ sở

Các mối phụ thuộc: không có sự phụ thuộc nào

11.2.4.1 Các phần tử của nhà phát triển

11.2.4.1.1 ADV_FSP.1.1D

Nhà phát triển cần cung cấp đặc tả chức năng.

11.2.4.1.2 ADV_FSP.1.2D

Nhà phát triển cần cung cấp truy vết từ đặc tả chức năng đến các SFR.

11.2.4.2 Các phần tử nội dung và trình bày

11.2.4.2.1 ADV_FSP.1.1C

Đặc tả chức năng cần mô tả mục tiêu và phương pháp sử dụng cho mỗi TSFI của thực thi SFR và hỗ trợ SFR.

11.2.4.2.2 ADV_FSP.1.2C

Đặc tả chức năng cần xác định tất cả các tham số liên quan với mỗi TSFI của thực thi SFR và hỗ trợ SFR.

11.2.4.2.3 ADV_FSP.1.3C

Đặc tả chức năng cần cung cấp sở cứ cho việc phân nhóm rõ ràng của các giao diện như không can thiệp SFR.

11.2.4.2.4 ADV_FSP.1.4C

Truy vết cần chứng minh rằng truy vết SFR theo TSFI trong đặc tả chức năng.

11.2.4.3 Các phần tử hành động của đánh giá viên

11.2.4.3.1 ADV_FSP.1.1E

Đánh giá viên cần xác nhận rằng thông tin cung cấp sự phù hợp với tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

11.2.4.3.2 ADV_FSP.1.2E

Đánh giá viên cần quyết định rằng đặc tả chức năng được khởi tạo chính xác và hoàn toàn của các SFR.

11.2.5 ADV_FSP.2 Đặc tả chức năng thực thi an toàn

Các phụ thuộc: ADV_TDS.1 Thiết kế cơ sở

11.2.5.1 Phần tử hành động của nhà phát triển

11.2.5.1.1 ADV_FSP.2.1D

Nhà phát triển cần cung cấp đặc tả chức năng

11.2.5.1.2 ADV_FSP.2.2D

Nhà phát triển cần cung cấp truy vết từ đặc tả chức năng đến các SFR.

11.2.5.2 Các phần tử nội dung và trình bày

11.2.5.2.1 ADV_FSP.2.1C

Đặc tả chức năng cần biểu diễn toàn bộ TSF.

11.2.5.2.2 ADV_FSP.2.2C

Đặc tả chức năng cần mô tả mục tiêu và phương pháp sử dụng cho tất cả TSFI.

11.2.5.2.3 ADV_FSP.2.3C

Đặc tả chức năng cần xác định và mô tả tất cả các tham số liên quan đến mỗi TSFI.

11.2.5.2.4 ADV_FSP.2.4C

Với mỗi TSFI thực thi SFR, đặc tả chức năng cần mô tả các hành động thực thi SFR liên quan đến mỗi TSFI.

11.2.5.2.5 ADV_FSP.2.5C

Với các TSFI thực thi SFR, đặc tả chức năng cần mô tả các thông báo lỗi trực tiếp có kết quả từ xử lý liên quan với các hành động thực thi SFR.

11.2.5.2.6 ADV_FSP.2.6C

Truy vết cần chứng minh rằng truy vết SFR từ các TSFI theo các đặc tả chức năng.

11.2.5.3 Các phần tử hành động của đánh giá viên

11.2.5.3.1 ADV_FSP.2.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày các bằng chứng.

11.2.5.3.2 ADV_FSP.2.2E

Đánh giá viên cần quyết định rằng các đặc tả chức năng là một sự khởi tạo chính xác và hoàn toàn của các SFR.

11.2.6 ADV_FSP.3 Đặc tả chức năng với tóm tắt đầy đủ

Các phụ thuộc: ADV_TDS.1 Thiết kế cơ sở

11.2.6.1 Phần tử hành động của nhà phát triển

11.2.6.1.1 ADV_FSP.3.1D

Nhà phát triển cần cung cấp đặc tả chức năng.

11.2.6.1.2 ADV_FSP.3.2D

Nhà phát triển cần cung cấp truy vết từ đặc tả chức năng đến các SFR.

11.2.6.2 Các phần tử nội dung và trình bày

11.2.6.2.1 ADV_FSP.3.1C

Đặc tả chức năng cần biểu diễn đầy đủ TSF

11.2.6.2.2 ADV_FSP.3.2C

Đặc tả chức năng cần mô tả mục tiêu và phương pháp sử dụng cho tất cả TSFI.

11.2.6.2.3 ADV_FSP.3.3C

Đặc tả chức năng cần xác định và mô tả tất cả các tham số liên quan với mỗi TSFI.

11.2.6.2.4 ADV_FSP.3.4C

Với mỗi TSFI của thực thi SFR, đặc tả chức năng cần mô tả các hành động thực thi SFR liên quan với TSFI.

11.2.6.2.5 ADV_FSP.3.5C

Với mỗi TSFI thực thi SFR, đặc tả chức năng cần mô tả trực tiếp các thông báo lỗi thu được từ các kết quả và ngoại lệ liên quan đến các lệnh gọi của TSFI.

11.2.6.2.6 ADV_FSP.3.6

Đặc tả chức năng cần tóm tắt các hành động **hỗ trợ SFR và không can thiệp SFR** liên quan đến mỗi TSFI.

11.2.6.2.7 ADV_FSP.3.7C

Truy vết cần chứng minh rằng SFR truy vết từ TSFI trong đặc tả chức năng.

11.2.6.3 Các phần tử hành động của đánh giá viên

11.2.6.3.1 ADV_FSP.3.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày chứng cứ.

11.2.6.3.2 ADV_FSP.3.2E

Đánh giá viên cần quyết định rằng đặc tả chức năng là chính xác và đầy đủ của các SFR.

11.2.7 ADV_FSP.4 Đặc tả chức năng đầy đủ

Các phụ thuộc: ADV_TDS.1 Thiết kế cơ sở

11.2.7.1 Phần tử hành động của nhà phát triển

11.2.7.1.1 ADV_FSP.4.1D

Nhà phát triển cần cung cấp đặc tả chức năng.

11.2.7.1.2 ADV_FSP.4.2D

Nhà phát triển cần cung cấp truy vết từ đặc tả chức năng đến các SFR.

11.2.7.2 Các phần tử nội dung và trình bày

11.2.7.2.1 ADV_FSP.4.1C

Đặc tả chức năng cần biểu diễn đầy đủ TSF.

11.2.7.2.2 ADV_FSP.4.2C

Đặc tả chức năng cần mô tả mục tiêu và phương pháp sử dụng của tất cả TSFI.

11.2.7.2.3 ADV_FSP.4.3C

Đặc tả chức năng cần xác định và mô tả tất cả các tham số liên quan với mỗi TSFI.

11.2.7.2.4 ADV_FSP.4.4C

Đặc tả chức năng cần mô tả tất cả các hành động liên quan với mỗi TSFI.

11.2.7.2.5 ADV_FSP.4.5C

Đặc tả chức năng cần mô tả tất cả các thông báo lỗi trực tiếp mà có kết quả từ việc gọi đến mỗi TSFI.

11.2.7.2.6 ADV_FSP.4.6C

Truy vết cần chứng minh rằng các SFR truy vết TSFI trong đặc tả chức năng.

11.2.7.3 Các phần tử hành động của đánh giá viên

11.2.7.3.1 ADV_FSP.4.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày các chứng cứ.

11.2.7.3.2 ADV_FSP.4.2E

Đánh giá viên cần quyết định rằng đặc tả chức năng là chính xác và đầy đủ của các SFR.

11.2.8 ADV_FSP.5 Đặc tả chức năng bán chính thức đầy đủ với thông tin lỗi bổ sung

Các phụ thuộc: ADV_TDS.1 Thiết kế cơ sở

ADV_IMP.1 Biểu diễn thực hiện của TSF.

11.2.8.1 Phần tử hành động của nhà phát triển

11.2.8.1.1 ADV_FSP.5.1D

Nhà phát triển cần cung cấp đặc tả chức năng

11.2.8.1.2ADV_FSP.5.2D

Nhà phát triển cần cung cấp truy vết từ đặc tả chức năng đến các SFR.

11.2.8.2 Các phần tử nội dung và trình bày

11.2.8.2.1ADV_FSP.5.1C

Đặc tả chức năng cần biểu diễn hoàn toàn TSF.

11.2.8.2.2ADV_FSP.5.2C

Đặc tả chức năng cần mô tả TSFI sử dụng kiểu bán hình thức.

11.2.8.2.3ADV_FSP.5.3C

Đặc tả chức năng cần mô tả mục tiêu và phương pháp sử dụng cho tất cả TSFI.

11.2.8.2.4ADV_FSP.5.4C

Đặc tả chức năng cần xác nhận và mô tả tất cả các tham số liên quan với mỗi TSFI.

11.2.8.2.5ADV_FSP.5.5C

Đặc tả chức năng cần mô tả tất cả các hành động liên quan đến mỗi TSFI.

11.2.8.2.6ADV_FSP.5.6C

Đặc tả chức năng cần mô tả tất cả các thông báo lỗi trực tiếp mà có kết quả từ việc gọi đến từ mỗi TSFI.

11.2.8.2.7ADV_FSP.5.7C

Đặc tả chức năng cần mô tả tất cả các thông báo lỗi mà không phải được gọi đến từ TSFI.

11.2.8.2.8ADV_FSP.5.8C

Đặc tả chức năng cần cung cấp sở cứ cho mỗi thông báo lỗi chứa trong thực hiện TSF nhưng kết quả không phải từ lệnh gọi đến TSFI.

11.2.8.2.9ADV_FSP.5.9C

Truy vết cần chứng minh rằng SFR truy vết đến các TSFI trong các đặc tả chức năng.

11.2.8.3 Các phần tử hành động của đánh giá viên

11.2.8.3.1ADV_FSP.5.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày các chứng cứ.

11.2.8.3.2 ADV_FSP.5.2E

Đánh giá viên cần quyết định rằng đặc tả chức năng là đầy đủ và chính xác của các SFR.

11.2.9 ADV_FSP.6 Đặc tả chức năng bán chính thức đầy đủ với đặc tả chính thức bổ sung

Các phụ thuộc: ADV_TDS.1 Thiết kế cơ sở

ADV_IMP.1 Biểu diễn thực hiện của TSF

11.2.9.1 Phần tử hành động của nhà phát triển

11.2.9.1.1 ADV_FSP.6.1D

Nhà phát triển cần cung cấp đặc tả chức năng.

11.2.9.1.2 ADV_FSP.6.2D

Nhà phát triển cần cung cấp biểu diễn chính thức của đặc tả chức năng của TSF.

11.2.9.1.3 ADV_FSP.6.3D

Nhà phát triển cần cung cấp truy vết từ đặc tả chức năng đến các SFR.

11.2.9.2 Các phần tử nội dung và trình bày

11.2.9.2.1 ADV_FSP.6.1C

Đặc tả chức năng cần biểu diễn đầy đủ TSF.

11.2.9.2.2 ADV_FSP.6.2C

Đặc tả chức năng cần mô tả TSFI sử dụng kiểu chính thức.

11.2.9.2.3 ADV_FSP.6.3C

Đặc tả chức năng cần mô tả mục tiêu và phương pháp sử dụng tất cả TSFI.

11.2.9.2.4 ADV_FSP.6.4C

Đặc tả chức năng cần chỉ ra và mô tả tất cả các tham số liên quan với mỗi TSFI.

11.2.9.2.5 ADV_FSP.6.5C

Đặc tả chức năng cần mô tả tất cả các hành động liên quan đến mỗi TSFI.

11.2.9.2.6 ADV_FSP.6.6C

Đặc tả chức năng cần mô tả tất cả các thông báo lỗi trực tiếp mà kết quả từ lệnh gọi của mỗi TSFI.

11.2.9.2.7 ADV_FSP.6.7C

Đặc tả chức năng cần mô tả tất cả thông báo lỗi chứa trong **biểu diễn thực hiện TSF**.

11.2.9.2.8 ADV_FSP.6.8C

Đặc tả chức năng cần cung cấp các sở cứ cho mỗi thông báo lỗi chứa trong việc thực hiện TSF mà **không được mô tả trong việc giải trình vì sao đặc tả chức năng không liên quan với TSFI.**

11.2.9.2.9 ADV_FSP.6.9C

Trình bày chính thức của các đặc tả chức năng của TSF cần mô tả TSF sử dụng kiểu chính thức, hỗ trợ bởi các văn bản giải thích không chính thức tại các nơi phù hợp.

11.2.9.2.10 ADV_FSP.6.10C

Truy vết cần chứng minh rằng SFR truy vết TSFI trong đặc tả chức năng.

11.2.9.3 Các phần tử hành động của đánh giá viên

11.2.9.3.1 ADV_FSP.6.1E

Đánh giá viên cần xác nhận rằng các thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

11.2.9.3.2 ADV_FSP.6.2E

Đánh giá viên cần quyết định rằng đặc tả chức năng là đầy đủ và chính xác với SFR.

11.3 Biểu diễn triển khai (ADV_IMP)

11.3.1 Mục tiêu

Chức năng của họ biểu diễn triển khai (ADV_IMP) là cho nhà phát triển làm sẵn sàng biểu diễn triển khai (và, ở mức độ cao hơn, việc tự thực hiện) của TOE trong một hình thức có thể được phân tích bằng đánh giá viên. Biểu diễn triển khai được sử dụng trong các hoạt động phân tích cho các họ khác (ví dụ, phân tích thiết kế TOE) để chứng minh rằng TOE sự phù hợp thiết kế của nó và để cung cấp một cơ sở cho việc phân tích ở các vùng khác của đánh giá (ví dụ, việc tìm kiếm các điểm yếu). Các biểu diễn triển khai được chờ đợi ở dưới dạng để chụp các hoạt động nội bộ chi tiết của TSF. Đây có thể là mã nguồn phần mềm, mã nguồn phần sụn, sơ đồ phần cứng và / hoặc thiết kế phần cứng IC mã ngôn ngữ hoặc dữ liệu lớp.

11.3.2 Phân mức thành phần

Thành phần trong họ này được phân mức dựa trên số lượng thực hiện được ánh xạ vào mô tả thiết kế TOE.

11.3.3 Chú thích ứng dụng

Sơ đồ mã nguồn hoặc phần cứng và/hoặc thiết kế phần cứng IC mã ngôn ngữ hoặc bố trí dữ liệu được sử dụng để xây dựng phần cứng thực tế là những ví dụ của các bộ phận của biểu diễn triển khai. Điều quan trọng cần lưu ý rằng trong khi các biểu diễn triển khai phải được sẵn sàng cho đánh giá viên, điều này không có nghĩa là đánh giá viên cần phải sở hữu đại diện đó. Ví dụ, nhà phát triển có thể yêu cầu đánh giá viên xem xét lại các biểu diễn triển khai tại một trang web lựa chọn của nhà phát triển.

Các biểu diễn triển khai toàn bộ được sẵn sàng để đảm bảo rằng các hoạt động phân tích không được rút ngắn do thiếu thông tin. Tuy vậy, điều này không có hàm ý rằng tất cả các đại diện được xem xét khi thực hiện phân tích các hoạt động đang được thực hiện. Điều này không thực tế ở hầu hết các trường hợp, thêm vào đó là nó rất có thể sẽ không dẫn đến một TOE có mức đảm bảo cao hơn so với mẫu mục tiêu của biểu diễn triển khai. Biểu diễn triển khai được làm sẵn để cho phép phân tích các phân tích phân rã thiết kế TOE khác (ví dụ như chức tả chức năng, thiết kế TOE), và để đạt được sự tin cậy mà các chức năng an toàn được mô tả ở mức độ cao hơn trong việc thiết kế thực sự xuất hiện để được thực hiện trong TOE.

Quy ước trong một số dạng của các biểu diễn triển khai có thể làm cho nó khó hoặc không thể xác định từ chính các biểu diễn triển khai những gì kết quả thực tế của việc biên dịch hoặc thông dịch thời gian thực. Ví dụ, chỉ thị, trình biên dịch cho các trình biên dịch ngôn ngữ C sẽ là nguyên nhân để các trình biên dịch loại trừ hoặc bao gồm toàn bộ các phần của mã này. Vì lý do này, điều quan trọng là các công cụ cung cấp "thêm" thông tin hoặc công cụ liên quan (kịch bản, trình biên dịch, vv) được cung cấp để các biểu diễn triển khai có thể được xác định chính xác.

Mục đích của các ánh xạ giữa các biểu diễn triển khai và mô tả thiết kế TOE là để trợ giúp phân tích của đánh giá viên. Các hoạt động nội bộ của TOE có thể được hiểu rõ hơn khi thiết kế TOE được phân tích với các phần tương ứng của biểu diễn triển khai.Lập bản đồ phục vụ như một chỉ mục trong các biểu diễn triển khai. Tại các thành phần thấp hơn, chỉ có một tập hợp con của các biểu diễn triển khai được ánh xạ tới các mô tả thiết kế TOE. Bởi vì sự không chắc chắn trong đó phần của biểu diễn triển khai sẽ cần ánh xạ như thế, nhà phát triển có thể chọn một trong hai ánh xạ đến biểu diễn triển khai

toàn bộ trước, hoặc phải chờ đợi để xem những phần của biểu diễn triển khai, đánh giá viên yêu cầu để được ánh xạ.

Các biểu diễn triển khai được thao tác bởi nhà phát triển dưới các hình thức thích hợp cho chuyển đổi để thực hiện trong thực tế. Ví dụ, nhà phát triển có thể làm việc với các tập tin có chứa mã nguồn, mà là cuối cùng đã được biên dịch để trở thành một phần của TSF. Nhà phát triển làm cho biểu diễn triển khai sẵn sàng dưới dạng để sử dụng bởi nhà phát triển, do đó đánh giá viên có thể sử dụng kỹ thuật tự động trong phân tích. Điều này cũng làm tăng sự tin cậy rằng việc kiểm tra các biểu diễn triển khai thực sự là một trong những sử dụng trong sản xuất của các TSF (như trái ngược với các trường hợp được cung cấp theođịnh dạng trình bày thay thế, như một phần mềm xử lý văn bản). Cần lưu ý rằng các hình thức khác của các biểu diễn triển khai cũng có thể được sử dụng bởi nhà phát triển, các mẫu này được cung cấp. Mục tiêu tổng thể là để cung cấp cho đánh giá viên với các thông tin sẽ phát huy tối đa hiệu quả của các nỗ lực phân tích của đánh giá viên.

Một số hình thức của biểu diễn triển khai có thể yêu cầu thêm thông tin, bởi vì họ giới thiệu những rào cản đáng kể cho sự hiểu biết và phân tích. Ví dụ như mã nguồn "bị che khuất" hoặc mã nguồn đã được làm cho khó hiểu theo những cách khác do đó nó ngăn cản sự hiểu biết và/hoặc phân tích. Các dạng biểu diễn triển khai thường do kết quả của nhà phát triển TOE đưa ra một phiên bản của biểu diễn triển khai và chạy một chương trình bị che khuất hay làm cho khó hiểu trong đó. Trong khi đại diện bị che khuất là những gì được biên dịch và có thể được gần hơn để thực hiện (về mặt cấu trúc) so với ban đầu, đại diện bị làm cho khó hiểu, cung cấp mã khó hiểu có thể tiêu tốn thời gian đáng kể khi thực hiện việc phân tích liên quan đến đại diện. Khi các hình thức biểu diễn được tạo ra, các thành phần yêu cầu chi tiết về các công cụ liệm / thuật toán che khuất được sử dụng để đại diện không bị che khuất có thể được cung cấp, và các thông tin bổ sung có thể được sử dụng để đạt được sự tin cậy về tiến trình che khuất không làm tổn hại bất kỳ chức năng an toàn nào.

11.3.4 ADV_IMP.1 Biểu diễn triển khai của TSF

Các phụ thuộc: ADV_TDS.3 Thiết kế mô đun cơ sở

ALC_TAT.1 Các công cụ phát triển được xác định rõ ràng

11.3.4.1 Phần tử hành động của nhà phát triển

11.3.4.1.1 ADV_IMP.1.1D

Nhà phát triển cần tạo ra sự sẵn sàng của biểu diễn triển khai cho toàn bộ TSF.

11.3.4.1.2 ADV_IMP.1.2D

Nhà phát triển cần cung cấp ánh xạ giữa mô tả thiết kế TOE và ví dụ của biểu diễn triển khai.

11.3.4.2 Các phần tử nội dung và trình bày

11.3.4.2.1 ADV_IMP.1.1C

Biểu diễn triển khai cần định nghĩa TSF theo một mức độ chi tiết như TSF có thể được tạo ra mà không cần các quyết định thiết kế thêm nào.

11.3.4.2.2 ADV_IMP.1.2C

Biểu diễn triển khai cần dưới dạng được sử dụng bởi các các cá nhân phát triển.

11.3.4.2.3 ADV_IMP.1.3C

Ánh xạ giữa mô tả thiết kế TOE và ví dụ thực hiện cần chứng minh sự đáp ứng của nó.

11.3.4.3 Các phần tử hành động của đánh giá viên

11.3.4.3.1 ADV_IMP.1.1E

Đánh giá viên cần xác nhận rằng, với các mẫu được lựa chọn của biểu diễn triển khai, thông tin được cung cấp đáp ứng tất cả nội dung và trình bày các chứng cứ.

11.3.5 ADV_IMP.2 Ánh xạ đầy đủ của biểu diễn triển khai của TSF.

Các phụ thuộc: ADV_TDS.3 Thiết kế mô dun cơ sở

ALC_TAT.1 Các công cụ phát triển được định nghĩa rõ ràng

ALC_CMC.5 Hỗ trợ nâng cao

11.3.5.1 Các hành động của nhà phát triển

11.3.5.1.1 ADV_IMP.2.1D

Nhà phát triển cần tạo ra biểu diễn triển khai sẵn sàng cho toàn bộ TSF.

11.3.5.1.2 ADV_IMP.2.2D

Nhà phát triển cần cung cấp ánh xạ giữa mô tả thiết kế TOE và toàn bộ biểu diễn triển khai.

11.3.5.2 Các phần tử nội dung và trình bày

11.3.5.2.1 ADV_IMP.2.1C

Biểu diễn thực hiện cần xác định TSF theo các mức chi tiết mà TSF có thể được tạo ra mà không cần các quyết định thiết kế thêm.

11.3.5.2.2 ADV_IMP.2.2C

Biểu diễn triển khai cần được định dạng dưới dạng được bởi nhà phát triển.

11.3.5.2.3 ADV_IMP.2.3C

Ánh xạ giữa mô tả thiết kế TOE và toàn bộ biểu diễn triển khai cần chứng minh sự đáp ứng.

11.3.5.3 Các phần tử hành động của đánh giá viên

11.3.5.3.1 ADV_IMP.2.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày các chứng cứ.

11.4 Nội bộ TSF (ADV_INT)

11.4.1 Mục tiêu

Họ này đề cập đến việc đánh giá cấu trúc trong của TSF. Một TSF có bản chất được cấu trúc rõ ràng sẽ dễ dàng hơn để thực hiện và ít có khả năng chứa lỗ hổng mà có thể dẫn đến các điểm yếu, nó cũng dễ dàng hơn để duy trì không cần đưa vào các lỗ hổng.

11.4.2 Phân mức thành phần

Các thành phần trong họ này này được phân mức trên cơ sở số lượng cấu trúc và giảm thiểu độ phức tạp cần thiết. Tập con được cấu trúc rõ rang ADV_INT.1 của các chỗ bản chất TSF yêu cầu bản chất được cấu trúc rõ ràng trên chỉ các phần lựa chọn của TSF. Thành phần này không bao gồm trong EAL bởi vì thành phần này được xem để sử dụng trong các trường hợp đặc biệt (ví dụ, người tài trợ có một

mối quan tâm cụ thể về một mô-đun mã hóa, mà bị cô lập với phần còn lại của TSF) và sẽ không được áp dụng rộng rãi. Ở mức độ tiếp theo, các yêu cầu về bản chất được cấu trúc rõ ràng được đặt trên toàn bộ TSF. Cuối cùng, giảm thiểu độ phức tạp được giới thiệu trong các thành phần cao nhất.

11.4.3 Chú thích ứng dụng

Những yêu cầu này, khi áp dụng cho các cấu trúc bên trong của TSF, thường dẫn đến những cải thiện mà hỗ trợ cả nhà phát triển và đánh giá viên trong sự hiểu biết về TSF, và cũng cung cấp cơ sở cho việc thiết kế và đánh giá các bộ kiểm thử. Hơn nữa, nâng cao hiểu biết của các TSF sẽ hỗ trợ nhà phát triển đơn giản hóa bảo trì nó.

Các yêu cầu trong họ này được trình bày ở mức độ khá trừu tượng. Sự đa dạng của TOE làm cho nó không thể biên soạn thành bất cứ điều gì cụ thể hơn là "có cấu trúc rõ ràng" hay "phức tạp tối thiểu". Sự biên minh về cấu trúc và tính phức tạp được chờ đợi được cung cấp từ các kỹ thuật đặc biệt được sử dụng trong các TOE. Ví dụ, phần mềm có thể được xem xét cấu trúc rõ ràng khi nó thể hiện những đặc điểm được trích dẫn trong các ngành kỹ nghệ phần mềm. Các thành phần bên trong họ này gọi để xác định các tiêu chuẩn để đo các tính chất được cấu trúc tốt và không quá phức tạp.

11.4.4 ADV_INT.1 Tập con cấu trúc rõ ràng của nội bộ TSF

Các phụ thuộc: ADV_IMP.1 Biểu diễn triển khai của TSF

ADV_TDS.3 Thiết kế mô đun cơ sở

ALC_TAT.1 Các công cụ phát triển được định nghĩa rõ ràng

11.4.4.1 Các mục tiêu

Mục tiêu của thành phần này là cung cấp theo cách làm cho việc yêu cầu các phần đặc biệt của TSF được cấu trúc rõ ràng.

Theo dự định toàn bộ TSF đã được thiết kế và thực hiện bằng cách sử dụng các nguyên tắc kỹ thuật phù hợp, nhưng phân tích được thực hiện dựa trên một tập con cụ thể.

11.4.4.2 Chú thích ứng dụng

Thành phần này yêu cầu tác giả PP và ST sẽ được gán đầy đủ với các tập con của TSF. Tập con này sẽ được xác định theo dạng bên trong của TSF tại bất kỳ lớp trừu tượng nào. Ví dụ:

a) các phần tử cấu trúc của TSF được xác định trong thiết kế TOE (ví dụ: "Nhà phát triển cần thiết kế và thực hiện kiểm tra hệ thống con theo cách mà nó có bản chất cấu trúc rõ ràng.")

b) thực hiện (ví dụ: "nhà phát triển cần thiết kế và thực hiện các tập tin encrypt.c và decrypt.c theo cách chúng có bản chất cấu trúc rõ ràng." hoặc "Nhà phát triển cần thiết kế và thực hiện chíp vi mạch 6.227 theo cách mà nó có bản chất cấu trúc rõ ràng". ")

Điều này dường như chưa sẵn sàng thực hiện bằng cách tham khảo các tuyên bố SFR (ví dụ: "Nhà phát triển cần thiết kế và thực hiện phần của TSF để cung cấp khả năng nặc danh như được định nghĩa trong FPR_ANO.2 như vậy mà nó có bản chất cấu trúc rõ ràng.") Bởi vì điều này không chỉ ra nơi tập trung phân tích.

Thành phần này có giá trị giới hạn và sẽ thích hợp trong trường hợp mà người sử dụng/chủ thể của các mã độc hại bị hạn chế hoặc truy cập kiểm soát truy nhập chặt chẽ các TSFI hoặc nơi có phương tiện bảo vệ khác (ví dụ, miền tách) để đảm bảo tập con được lựa chọn của TSF không thể bị ảnh hưởng bởi phần còn lại của TSF (ví dụ, các chức năng mã hóa, mà bị cô lập với phần còn lại của TSF, có cấu trúc rõ ràng).

11.4.4.3 Phần tử hành động của nhà phát triển

11.4.4.3.1 ADV_INT.1.1D

Nhà phát triển cần thiết kế và thực hiện [gán: tập con của TSF] theo đó nó có bản chất được cấu trúc rõ ràng.

11.4.4.3.2 ADV_INT.1.2D

Nhà phát triển cần cung cấp mô tả và biện minh cho nội bộ.

11.4.4.4 Các phần tử nội dung và trình bày

11.4.4.4.1 ADV_INT.1.1C

Biện minh cần giải thích các bản chất được sử dụng để xem xét ý nghĩa của "cấu trúc rõ ràng".

11.4.4.4.2 ADV_INT.1.2C

Mô tả các tính chất TSF cần chứng minh rằng tập con được gán của TSF là được cấu trúc rõ ràng.

11.4.4.5 Các phần tử hành động của đánh giá viên

11.4.4.5.1 ADV_INT.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

11.4.4.5.2 ADV_INT.1.2E

Đánh giá viên cần thực hiện phân tích bản chất dựa trên các tập con được gán của TSF.

11.4.5 ADV_INT.2 Nội bộ với cấu trúc rõ ràng

Các phụ thuộc: ADV_IMP.1 Biểu diễn triển khai của TSF.

ADV_TDS.3 Thiết kế mô đun cơ sở

ALC_TAT.1 Các công cụ phát triển được định nghĩa rõ ràng.

11.4.5.1 Mục tiêu

Mục tiêu của thành phần này là cung cấp theo cách làm cho việc yêu cầu TSF được cấu trúc rõ ràng. Theo dự định toàn bộ TSF đã được thiết kế và thực hiện bằng cách sử dụng các nguyên tắc kỹ thuật phù hợp.

11.4.5.2 Chú thich ứng dụng

Sự biện minh về tính đầy đủ của cấu trúc và sự phức tạp được chờ đợi sẽ nhận được từ kỹ thuật đặc biệt được sử dụng trong TOE. Thành phần này gọi để xác định các tiêu chuẩn để đo đạc tính chất của các cấu trúc rõ ràng.

11.4.5.3 Phần tử hành động của nhà phát triển

11.4.5.3.1 ADV_INT.2.1D

Nhà phát triển cần thiết kế và thực hiện toàn bộ TSF mà bản chất có cấu trúc rõ ràng.

11.4.5.3.2 ADV_INT.2.2D

Nhà phát triển cần cung cấp mô tả và biện minh cho bản chất.

11.4.5.4 Các phần tử nội dung và trình bày

11.4.5.4.1 ADV_INT.2.1C

Sự biện minh cần mô tả các tính chất sử dụng để xem xét ý nghĩa của "cấu trúc rõ ràng".

11.4.5.4.2 ADV_INT.2.2C

Mô tả bản chất TSF cần chứgn minh rằng toàn bộ TSF có cấu trúc rõ ràng.

11.4.5.5 Các phần tử hành động của đánh giá viên

11.4.5.5.1 ADV_INT.2.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng đầy đủ các yêu cầu cho nội dung và trình bày chứng cứ.

11.4.5.5.2 ADV_INT.2.2E

Đánh giá viên cần thực hiện phân tích bản chất bên trong TSF.

11.4.6 ADV_INT.3 Nội bộ với độ phức tạp tối thiểu

Các phụ thuộc: ADV_IMP.1 Biểu diễn triển khai của TSF

ADV_TDS.3 Thiết kế mô dun cơ sở

ALC_TAT.1 Các công cụ phát triển được định nghĩa rõ ràng

11.4.6.1 Mục tiêu

Mục tiêu của thành phần này là cung cấp theo cách làm cho việc yêu cầu TSF được cấu trúc rõ ràng và sự phức tạp nhỏ nhất. Theo dự định toàn bộ TSF đã được thiết kế và thực hiện bằng cách sử dụng các nguyên tắc kỹ thuật phù hợp.

11.4.6.2 Chú thích ứng dụng

Sự biện minh về tính đầy đủ của cấu trúc và sự phức tạp được chờ đợi sẽ nhận được từ kỹ thuật đặc biệt được sử dụng trong TOE. Thành phần này gọi để xác định các tiêu chuẩn để đo đạc cấu trúc và độ phức tạp.

11.4.6.3 Phần tử hành động của nhà phát triển

11.4.6.3.1 ADV_INT.3.1D

Nhà phát triển cần thiết kế và thực hiện toàn bộ TSF mà bản chất được cấu trúc rõ ràng.

11.4.6.3.2 ADV_INT.3.2D

Nhà phát triển cần cung cấp mô tả và biện minh cho bản chất..

11.4.6.4 Các phần tử nội dung và trình bày

11.4.6.4.1 ADV_INT.3.1C

Sự biện minh cần mô tả các tính chất được sử dụng để xem xét ý nghĩa của "Cấu trúc rõ ràng" và **"phức tạp".**

11.4.6.4.2 ADV_INT.3.2C

Mô tả các bản chất của TSF cần chứng minh rằng thảon bộ TSF được cấu trúc rõ ràng và không phức tạp quá.

11.4.6.5 Các phần tử hành động của đánh giá viên

11.4.6.5.1 ADV_INT.3.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu cho nội dung và trình bày các chứng cứ.

11.4.6.5.2 ADV_INT.3.2E

Đánh giá viên cần thực hiện phân tích bản chất của trên toàn TSF.

11.5 Mô hình hóa chính sách an toàn (ADV_SPM)

11.5.1 Mục tiêu

Mục tiêu của họ này là cung cấp sự bảo đảm bổ sung từ sự phát triển của một mô hình chính sách an toàn chính thức của TSF, và thiết lập một sự tương ứng giữa các đặc tả chức năng và mô hình chính sách an toàn. Bảo vệ sự nhất quan nội bộ mô hình chính sách an toàn được chờ đợi để thiết lập các nguyên tắc an toàn từ các tính chất của nó bằng một chứng minh toán học.

11.5.2 Phân mức thành phần

Họ này chứa chỉ một thành phần.

11.5.3 Chú thích ứng dụng

Bất cập trong một TOE có thể dẫn đến kết quả là thất bại trong việc tìm hiểu các yêu cầu an toàn và, từ một thiếu sót trong thực hiện các yêu cầu an toàn. Việc xác định các yêu cầu an toàn đầy đủ để đảm bảo sự hiểu biết của họ có thể có vấn đề bởi vì các định nghĩa cần phải đủ chính xác để tránh kết quả không mong muốn hoặc sai sót trong quá trình thực hiện của TOE. Qua việc thực hiện, thiết kế, và quy trình soát xét, các yêu cầu bảo vệ được mô hình hóa có thể được sử dụng như là thiết kế chính xác và hướng dẫn thực hiện, qua đó cung cấp đảm bảo tăng lên đáp ứng các yêu cầu an toàn được thỏa mãn bởi TOE. Độ chính xác của mô hình và kết quả hướng dẫn là dấu hiệu cải thiện đáng kể bằng việc tạo các mô hình trong một ngôn ngữ chính thức và xác minh các yêu cầu an toàn bởi chứng minh hình thức.

Việc tạo ra một mô hình chính sách an toàn chính thức giúp xác định và loại bỏ các phần tử chính sách an toàn không rõ ràng, không phù hợp, mâu thuẫn, hoặc không thể thực thi. Chỉ khi TOE đã được xây dựng, mô hình chính thức phục vụ các nỗ lực đánh giá góp phần cho các phán xét của đánh giá viên về việc nhà phát triển có hiểu biết thế nào về chức năng an toàn đang được thực hiện và có sự nhất quán giữa yêu cầu an toàn và thiết kế TOE. Sự tin cậy trong mô hình này được đi kèm với bằng chứng rằng nó không chứa mâu thuẫn.

Mô hình chính sách an toàn chính thức là một bài thuyết trình chính thức chính xác về các khía cạnh quan trọng của an toàn và mối quan hệ của chúng với các hành vi của TOE, nó xác định tập các quy tắc và thông lệ điều chỉnh làm thế nào TSF quản lý, bảo vệ, và kiểm soát các tài nguyên hệ thống. Mô hình này bao gồm việc thiết lập các hạn chế và các thuộc tính mà chỉ ra làm thế nào thông tin và tài nguyên tính toán bị ngăn không cho sử dụng khi vi phạm các SFR, kèm theo một tập thuyết phục các đối số kỹ thuật cho thấy rằng những hạn chế này và các thuộc tính đóng một vai trò quan trọng trong việc thực thi SFR . Nó bao gồm cả hình thức hóa mà biểu diễn các chức năng an toàn, cũng như các văn bản phụ trợ để giải thích các mô hình và cung cấp cho nó với ngữ cảnh. Các hành vi an toàn của TSF được mô hình hóa cả về hành vi bên ngoài (tức là làm thế nào TSF tương tác với phần còn lại của TOE và với môi trường hoạt động của nó), cũng như các hành vi nội bộ của nó.

Các mô hình chính sách an toàn của TOE được trích dẫn không chính thức từ thực tế của nó bằng cách xem xét các yêu cầu an toàn được đề nghị của ST này. Việc trích dẫn không chính thức được thực hiện thành công nếu các nguyên tắc của TOE (còn gọi là "bất biến") đưa ra được thực thi bởi các đặc tính của nó. Mục đích của các phương pháp chính thức nằm trong việc tăng cường sự chặt chẽ của việc thực thi. Đối số không chính thức luôn dễ bị sai lầm, đặc biệt là nếu các mối quan hệ giữa các chủ thể, đối tượng và hoạt động nhận được thamg gia nhiều hơn và nhiều hơn nữa. Để giảm thiểu nguy cơ về trạng thái không an toàn đưa đến các quy tắc và tính chất của mô hình chính sách an toàn được ánh xạ tới các thuộc tính tương ứng và các đặc trưng bên trong một số hệ thống chính thức, với sự chặt chẽ và mạnh mẽ có thể được sử dụng sau đó để có được các thuộc tính an toàn qua các định lý và bằng chứng chính thức.

Trong khi thuật ngữ "mô hình chính sách an toàn chính thức" được sử dụng trong giới học thuật, cách tiếp cận của TCVN 8709 không có nghĩa cố định về "an toàn", nó sẽ tương đương với bất cứ điều gì SFR được tuyên bố. Vì vậy, mô hình chính sách an toàn chính thức chỉ là một đại diện chính thức của tập SFR được tuyên bố.

Các chính sách an toàn có kết hợp truyền thống chỉ với chính sách kiểm soát truy cập, mà dựa trên nhãn (bắt buộc kiểm soát truy cập), hoặc dựa trên người dùng (kiểm soát truy cập tùy ý). Tuy nhiên, một chính sách an toàn không giới hạn kiểm soát truy cập, còn có những chính sách kiểm tra, chính sách xác định, chính sách xác thực, chính sách mã hóa, chính sách quản lý, và các chính sách an toàn khác mà được thực thi bởi các TOE, như mô tả trong PP/ST. ADV_SPM.1.1D chứa phần để xác định các chính sách này được mô hình hóa chính thức.

11.5.4 ADV_SPM.1 Mô hình chính sách an toàn TOE chính thức

Các phụ thuộc: ADV_FSP.4 Đặc tả chức năng đầy đủ.

11.5.4.1 Phần tử hành động của nhà phát triển

11.5.4.1.1 ADV_SPM.1.1D

Nhà phát triển cần cung cấp mô hình chính sách an toàn chính thức cho [gán: dánh sách các chính sách mà được mô hình hóa chính thức].

11.5.4.1.2 ADV_SPM.1.2D

Mỗi chính sách bao gồm mô hình chính sách an toàn chính thức, mô hình này cần chỉ ra các phần phù hợp của tuyên bố của SFR mà là sự phối hợp chính sách đó.

11.5.4.1.3 ADV_SPM.1.3D

Nhà phát triển cần cung cấp chứng minh chính thức về sự tương ứng giữa mô hình và bất kỳ đặc tả chức năng chính thức nào.

11.5.4.1.4 ADV_SPM.1.4D

Nhà phát triển cần cung cấp chứng minh sự tương ứng giữa mô hình và đặc tả chức năng.

11.5.4.2 Các phần tử nội dung và trình bày

11.5.4.2.1 ADV_SPM.1.1C

Mô hình cần cung cấp kiểu chính thức, được hỗ trợ bởi văn bản giải thích được yêu cầu và xác định các chính sách an toàn của TSF được mô hình hóa.

11.5.4.2.2 ADV_SPM.1.2C

Tất cả các chính sách mà được mô hình hóa, mô hình cần định nghĩa an toàn cho TOE và cung cấp chứng minh chính thức mà TOE không thể tiếp cận đến trạng thái không an toàn.

11.5.4.2.3 ADV_SPM.1.3C

Sự phù hợp giữa mô hình và đặc tả chức năng cần ở mức chính xác của quy cách.

11.5.4.2.4 ADV_SPM.1.4C

Sự phù hợp cần chỉ ra đặc tả chức năng là nhất quán và đầy đủ với toàn bộ về mô hình.

11.5.4.2.5 ADV_SPM.1.5C

Chứng minh sự phù hợp cần chỉ ra rằng các giao diện trong đặc tả chức năng là nhất quan và đầy đủ về các chính sách được phân trong ADV_SPM.1.1D.

11.5.4.3 Các phần tử hành động của đánh giá viên

11.5.4.3.1 ADV_SPM.1.1E

Đánh giá viên cần xác nhận rằng thông tin được cung cấp đáp ứng đầy đủ tất cả các yêu cầu về nội dung và trình bày chứng cứ.

11.6 Thiết kế TOE (ADV_TDS)

11.6.1 Mục tiêu

Bản mô tả thiết kế cho một TOE đưa ra ngữ cảnh mô tả cho TSF đồng thời mô tả chi tiết cho TSF. Khi nhu cầu đảm bảo tăng, mức chi tiết trong mô tả cũng tăng. Khi phạm vi và độ phức tạp của TSF tăng, việc phân tách nhiều mức là thích hợp. Các yêu cầu thiết kế đưa ra các thông tin với chủ ý (tương xứng với mức đảm bảo cho trước) sao cho có thể đưa ra quyết định về việc các yêu cầu chức năng an toàn đã được thực hiện.

11.6.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở tổng số thông tin đòi hỏi phải thể hiện ứng với TSF và tùy vào mức độ hình thức yêu cầu của mô tả thiết kế.

11.6.3 Chú thích ứng dụng

Mục tiêu của tài liệu thiết kế là đưa ra thông tin đầy đủ để xác định ranh giới TSF và mô tả TSF triển khai các yêu cầu chức năng an toàn như thế nào. Số lượng và cấu trúc của tài liệu thiết kế phụ thuộc vào độ phức tạp của TOE và số các SFR. Thông thường, một TOE khá phức tạp với một lượng lớn SFR sẽ đòi hỏi nhiều tài liệu thiết kế hơn một TOE đơn giản chỉ triển khai cho một vài SFR. Các TOE phức tạp hơn sẽ được lợi từ việc tạo ra các mức phân tách khác nhau trong mô tả thiết kế, trong khi các TOE đơn giản hơn không đòi hỏi mô tả mức cao và mức thấp việc triển khai chúng.

Họ này có hai mức phân tách: hệ thống con và mô đun. Một mô đun là bản mô tả chức năng đặc trưng nhất, nó chính là bản mô tả triển khai. Một nhà phát triển cần có khả năng triển khai một phần TOE mô tả trong mô đun mà không cần thêm các giải trình về thiết kế khác. Một hệ thống con là bản mô tả thiết kế TOE, nó giúp đưa ra mô tả mức cao về một thành phần TOE đang làm gì và như thế nào. Do vậy, một hệ thống con có thể được chia ra các hệ thống con mức thấp hơn, hoặc chia ra thành các mô đun. Các TOE phức tạp có thể đòi hỏi một số mức hệ thống con khác nhau nhằm truyền đạt phù hợp thông tin mô tả hữu ích về việc TOE làm việc như thế nào. Các TOE đơn giản hơn thì ngược lại không đòi hỏi mô tả cấp hệ thống con nào, mô đun của nó có thể mô tả rõ ràng cách thức làm việc của TOE.

Cách thức chung cho tài liệu thiết kế là tùy theo mức độ đảm bảo tăng dần, mức độ chi tiết của mô tả đi từ mô tả chung (mức hệ thống con) đến mô tả chi tiết hơn (mức mô đun). Trong các trường hợp mức độ trừu tượng ở mức mô đun là phù hợp vì TOE đơn giản đủ để mô tả ở mức mô đun song mức đảm bảo yêu cầu mô tả ở mức hệ thống con, thì chỉ cần mô tả ở mức mô đun là đủ. Tuy nhiên, đối với các TOE phức tạp thì không phải như vậy: một lượng lớn các chi tiết (mức mô đun) cũng sẽ không đủ nếu không có kèm theo mô tả ở mức hệ thống con.

Phương thức này tuân theo một mô hình chung là cung cấp chi tiết bổ sung khi triển khai TSF sẽ đem lại sự đảm bảo tốt hơn về việc các SFR được thực thi chính xác và đưa ra thông tin sử dụng để biểu thị điều này trong kiểm thử (Kiểm thử ATE).

Trong các yêu cầu của họ này, khái niệm giao diện dùng để chỉ phương tiện trao đổi (giữa hai hệ thống con hoặc hai mô đun). Nó mô tả cách thức thực hiện trao đổi, tương tự như các chi tiết của TSFI (xem Đặc tả chức năng ADV_FSP). Khái niệm tương tác dùng để chỉ ra mục đích trao đổi, nó chỉ ra lý do hai hệ thống con hoặc hai mô đun trao đổi với nhau.

11.6.3.1 Chi tiết về các hệ thống con và các mô đun

Các yêu cầu xác định ra tập các chi tiết về các hệ thống con và các mô đun cần đưa ra gồm:

a) Các hệ thống con và các mô đun được xác định với một danh sách đơn giản mô tả chúng là những gì.

b) Các hệ thống con và các mô đun có thể được phân loại (rõ ràng hoặc ngầm định) thành "bắt buộc theo SFR", "Hỗ trợ SFR", hoặc "Không liên quan đến SFR". Các khái niệm này được dùng tương tự như trong phần đặc tả chức năng (ADV_FSP).

c) Hoạt động của một hệ thống con chỉ ra nó làm những gì. Hoạt động này có thể phân loại thành "bắt buộc theo SFR", "Hỗ trợ SFR", hoặc "Không liên quan đến SFR". Hoạt động của hệ thống con không bao giờ được phân loại khi phân ra nhiều SFR phù hợp hơn là phân loại hệ thống con. Ví dụ, một hệ thống con bắt buộc theo SFR có thể có hoạt động bắt buộc theo SFR và cũng có thể là hoạt động Hỗ trợ SFR hoặc Không liên quan đến SFR.

d) Tóm tắt hoạt động của một hệ thống con là một mô tả tổng quát về các hành động nó thực hiện (ví dụ "hệ thống con TCP tập hợp các IP datagram vào các luồng byte tin cậy").

e) Mô tả hoạt động của một hệ thống con là một bản giải thích về mọi điều nó làm. Mô tả này cần ở mức chi tiết để có thể xác định rõ ràng là hoạt động này có bất kỳ sự liên quan nào đến việc thực thi các SFR hay không.

f) Mô tả các tương tác của các hệ thống con và các mô đun hoặc tương tác giữa chúng chỉ ra lý do trao đổi thông tin giữa các hệ thống con hoặc các mô đun, và đặc tả thông tin chuyển qua nó. Không cần phải xác định thông tin chi tiết như đặc tả của một giao diện. Ví dụ, sẽ đủ khi nói rằng "hệ thống con X yêu cầu một khối bộ nhớ từ bộ quản lý bộ nhớ, và nhận được vị trí bộ nhớ đã cấp phát".

g) Mô tả giao diện cung cấp chi tiết về cách thức thực hiện các tương tác giữa các mô đun. Thay vì mô tả lý do các mô đun trao đổi với nhau hay mục đích việc trao đổi thông tin của chúng (nghĩa là mô tả các tương tác), mô tả giao diện mô tả chi tiết cách thức thực hiện trao đổi thông tin với các thuật ngữ về cấu trúc, nội dung các bản tin, đánh tín hiệu, các trao đổi tiến trình nội bộ,...

h) Mục đích mô tả phương thức một mô đun cung cấp chức năng của nó. Nó đưa ra chi tiết đủ để không cần phải thêm giải trình thiết kế nào khác. Cần thể hiện rõ tính phù hợp mô tả triển khai mô đun và mục đích của mô đun.

i) Một mô đun được mô tả theo các khác với các thuật ngữ được xác định trong phần tử của nó.

Các hệ thống con và các mô đun, khái niệm "Bắt buộc theo SFR", v.v. sẽ được giải thích chi tiết hơn trong Phụ lục A.4: Các hệ thống con và các mô đun: ADV_TDS

11.6.4 ADV_TDS. 1 Thiết kế cơ sở

Các phụ thuộc: ADV_FSP.2 Đặc tả chức năng thực thi an toàn

11.6.4.1 Phần tử hành động của nhà phát triển

11.6.4.1.1 ADV_TDS.1.1D

Nhà phát triển cần đưa ra được bản thiết kế của TOE.

11.6.4.1.2 ADV_TDS.1.2D

Nhà phát triển cần đưa ra được bản ánh xạ giữa TSFI về đặc tả chức năng và mức phân tách thấp nhất dùng được trong thiết kế TOE.

11.6.4.2 Các phần tử nội dung và trình bày

11.6.4.2.1 ADV_TDS.1.1C

Bản thiết kế cần mô tả cấu trúc TOE với các hệ thống con.

11.6.4.2.2 ADV_TDS.1.2C

Bản thiết kế cần chỉ ra tất cả các hệ thống con của TSF.

11.6.4.2.3 ADV_TDS.1.3C

Bản thiết kế cần mô tả hoạt động của mỗi hệ thống con TSF kiểu "hỗ trợ SFR" hoặc "không liên quan SFR" ở mức độ chi tiết đủ để khẳng định nó không phải là kiểu "bắt buộc theo SFR".

11.6.4.2.4 ADV_TDS.1.4C

Bản thiết kế cần tóm lược hoạt động bắt buộc theo SFR cho các hệ thống con kiểu "bắt buộc theo SFR".

11.6.4.2.5 ADV_TDS.1.5C

Bản thiết kế cần đưa ra mô tả về tương tác của các hệ thống con kiểu "bắt buộc theo SFR" của TSF, và giữa các hệ thống con đó với các hệ thống con của TSF khác.

11.6.4.2.6 ADV_TDS.1.6C

Bản thiết kế cần biểu thị rằng mọi hoạt động mô tả trong thiết kế TOE được ánh xạ vào trong các TSFI thực thi chúng.

11.6.4.3 Các phần tử hành động của đánh giá viên

11.6.4.3.1 ADV_TDS.1.1E

Đánh giá viên cần khẳng định rằng thông tin đã cung cấp đáp ứng mọi yêu cầu về nội dung và biểu thị bằng chứng.

11.6.4.3.2 ADV_TDS.1.2E

Đánh giá viên cần xác định rằng bản thiết kế là một bản sao chính xác và đầy đủ mọi yêu cầu chức năng an toàn.

11.6.5 ADV_TDS.2 Thiết kế kiến trúc

Các phụ thuộc: ADV_FSP.3 Đặc tả chức năng với bản tổng hợp đầy đủ

11.6.5.1 Phần tử hành động của nhà phát triển

11.6.5.1.1 ADV_TDS.2.1D

Nhà phát triển cần đưa ra được bản thiết kế của TOE.

11.6.5.1.2 ADV_TDS.2.2D

Nhà phát triển cần đưa ra được bản ánh xạ giữa TSFI về đặc tả chức năng và mức phân tách thấp nhất dùng được trong thiết kế TOE.

11.6.5.2 Các phần tử nội dung và trình bày

11.6.5.2.1 ADV_TDS.2.1C

Bản thiết kế cần mô tả cấu trúc TOE với các hệ thống con.

11.6.5.2.2 ADV_TDS.2.2C

Bản thiết kế cần chỉ ra tất cả các hệ thống con của TSF.

11.6.5.2.3 ADV_TDS.2.3C

Bản thiết kế cần mô tả hoạt động của mỗi hệ thống con TSF kiểu "không liên quan SFR" ở mức độ chi tiết đủ để khẳng định nó là kiểu "không liên quan SFR".

11.6.5.2.4 ADV_TDS.2.4C

Bản thiết kế cần tóm lược hoạt động bắt buộc theo SFR cho các hệ thống con kiểu "bắt buộc theo SFR".

11.6.5.2.5 ADV_TDS.2.5C

Bản thiết kế cần tóm tắt hoạt động "hỗ trợ SFR" và "không liên quan SFR" của các hệ thống con kiểu "bắt buộc theo SFR".

11.6.5.2.6 ADV_TDS.2.6C

Bản thiết kế cần tóm tắt hoạt động của các hệ thống con kiểu "hỗ trợ SFR".

11.6.5.2.7 ADV_TDS.2.7C

Bản thiết kế cần đưa ra mô tả về tương tác của tất cả các hệ thống con của TSF.

11.6.5.2.8 ADV_TDS.2.8C

Bản thiết kế cần biểu thị rằng mọi hoạt động mô tả trong thiết kế TOE được ánh xạ vào trong các TSFI thực thi chúng.

11.6.5.3 Các phần tử hành động của đánh giá viên

11.6.5.3.1 ADV_TDS.2.1E

Đánh giá viên cần khẳng định rằng thông tin đã cung cấp đáp ứng mọi yêu cầu về nội dung và biểu thị bằng chứng.

11.6.5.3.2 ADV_TDS.2.2E

Đánh giá viên cần xác định rằng bản thiết kế là một bản sao chính xác và đầy đủ mọi yêu cầu chức năng an toàn.

11.6.6 ADV_TDS.3 Thiết kế mô đun cơ sở

Các phụ thuộc: ADV_FSP.4 Đặc tả chức năng đầy đủ

11.6.6.1 Phần tử hành động của nhà phát triển

11.6.6.1.1 ADV_TDS.3.1D

Nhà phát triển cần đưa ra được bản thiết kế của TOE.

11.6.6.1.2 ADV_TDS.3.2D

Nhà phát triển cần đưa ra được bản ánh xạ giữa TSFI về đặc tả chức năng và mức phân tách thấp nhất dùng được trong thiết kế TOE.

11.6.6.2 Các phần tử nội dung và trình bày

11.6.6.2.1 ADV_TDS.3.1C

Bản thiết kế cần mô tả cấu trúc TOE với các hệ thống con.

11.6.6.2.2 ADV_TDS.3.2C

Bản thiết kế cần mô tả tất cả các mô đun của TSF.

11.6.6.2.3 ADV_TDS.3.3C

Bản thiết kế cần chỉ ra tất cả các hệ thống con của TSF.

11.6.6.2.4 ADV_TDS.3.4C

Bản thiết kế cần **đưa ra mô tả cho mỗi hệ thống con** của **TSF**.

11.6.6.2.5 ADV_TDS.3.5C

Bản thiết kế cần đưa ra mô tả cho các tương tác của mọi hệ thống con của TSF.

11.6.6.2.6 ADV_TDS.3.6C

Bản thiết kế cần đưa ra ánh xạ từ các hệ thống con của TSF đến các mô đun của TSF.

11.6.6.2.7 ADV_TDS.3.7C

Bản thiết kế cần mô tả mỗi mô đun **"hỗ trợ SFR" và "không liên quan SFR" với mục đích và tương tác của chúng với các mô đun khác.**

11.6.6.2.8 ADV_TDS.3.8C

Bản thiết kế cần mô tả mỗi mô đun "bắt buộc theo SFR" với các giao diện liên quan SFR của chúng, cho lại các giá trị từ các giao diện này, tương tác với và gọi các giao diện tới các mô đun khác.

11.6.6.2.9 ADV_TDS.3.9C

Bản thiết kế cần mô tả mỗi **mô đun "hỗ trợ SFR" hoặc "không liên quan SFR"** với mục đích và **tương tác của chúng với các mô đun khác.**

11.6.6.2.10 ADV_TDS.3.10C

Bản thiết kế cần biểu thị rằng mọi hoạt động mô tả trong thiết kế TOE được ánh xạ vào trong các TSFI thực thi chúng.

11.6.6.3 Các phần tử hành động của đánh giá viên

11.6.6.3.1 ADV_TDS.3.1E

Đánh giá viên cần khẳng định rằng thông tin đã cung cấp đáp ứng mọi yêu cầu về nội dung và biểu thị bằng chứng.

11.6.6.3.2 ADV_TDS.3.2E

Đánh giá viên cần xác định rằng bản thiết kế là một bản sao chính xác và đầy đủ mọi yêu cầu chức năng an toàn.

11.6.7 ADV_TDS.4 Thiết kế mô đun bán chính thức

Các phụ thuộc: ADV_FSP.5 Đặc tả chức năng bán chính thức đầy đủ với thông tin lỗi bổ sung

11.6.7.1 Phần tử hành động của nhà phát triển

11.6.7.1.1 ADV_TDS.4.1D

Nhà phát triển cần đưa ra được bản thiết kế của TOE.

11.6.7.1.2 ADV_TDS.4.2D

Nhà phát triển cần đưa ra được bản ánh xạ giữa TSFI về đặc tả chức năng và mức phân tách thấp nhất dùng được trong thiết kế TOE.

11.6.7.2 Các phần tử nội dung và trình bày

11.6.7.2.1 ADV_TDS.4.1C

Bản thiết kế cần mô tả cấu trúc TOE với các hệ thống con.

11.6.7.2.2 ADV_TDS.4.2C

Bản thiết kế cần mô tả TSF với các mô đun, thiết kế mỗi mô đun theo **"bắt buộc theo SFR", "hỗ trợ SFR", hoặc "không liên quan SFR"**.

11.6.7.2.3 ADV_TDS.4.3C

Bản thiết kế cần chỉ ra tất cả các hệ thống con của TSF.

11.6.7.2.4 ADV_TDS.4.4C

Bản thiết kế cần đưa ra mô tả **bán chính thức** cho mỗi hệ thống con của TSF, **với văn bản giải thích không chính thức phù hợp.**

11.6.7.2.5 ADV_TDS.4.5C

Bản thiết kế cần đưa ra mô tả cho các tương tác của mọi hệ thống con của TSF.

11.6.7.2.6 ADV_TDS.4.6C

Bản thiết kế cần đưa ra ánh xạ từ các hệ thống con của TSF đến các mô đun của TSF.

11.6.7.2.7 ADV_TDS.4.7C

Bản thiết kế cần mô tả mỗi mô đun **"bắt buộc SFR" và "hỗ trợ SFR"** với mục đích và tương tác của chúng với các mô đun khác.

11.6.7.2.8 ADV_TDS.4.8C

Bản thiết kế cần mô tả mỗi mô đun "bắt buộc theo SFR" với các giao diện liên quan SFR của chúng, cho lại các giá trị từ các giao diện này, tương tác với và gọi các giao diện tới các mô đun khác.

11.6.7.2.9 ADV_TDS.4.9C

Bản thiết kế cần mô tả mỗi mô đun "không liên quan SFR" với mục đích và tương tác của chúng với các mô đun khác.

11.6.7.2.10 ADV_TDS.4.10C

Bản thiết kế cần biểu thị rằng mọi hoạt động mô tả trong thiết kế TOE được ánh xạ vào trong các TSFI thực thi chúng.

11.6.7.3 Các phần tử hành động của đánh giá viên

11.6.7.3.1 ADV_TDS.4.1E

Đánh giá viên cần khẳng định rằng thông tin đã cung cấp đáp ứng mọi yêu cầu về nội dung và biểu thị bằng chứng.

11.6.7.3.2 ADV_TDS.4.2E

Đánh giá viên cần xác định rằng bản thiết kế là một bản sao chính xác và đầy đủ mọi yêu cầu chức năng an toàn.

11.6.8 ADV_TDS.5 Thiết kế mô đun bán chính thức đầy đủ

Các phụ thuộc: ADV_FSP.5 Đặc tả chức năng bán chính thức đầy đủ với thông tin lỗi bổ sung

11.6.8.1 Phần tử hành động của nhà phát triển

11.6.8.1.1 ADV_TDS.5.1D

Nhà phát triển cần đưa ra được bản thiết kế của TOE.

11.6.8.1.2 ADV_TDS.5.2D

Nhà phát triển cần đưa ra được bản ánh xạ giữa TSFI về đặc tả chức năng và mức phân tách thấp nhất dùng được trong thiết kế TOE.

11.6.8.2 Các phần tử nội dung và trình bày

11.6.8.2.1 ADV_TDS.5.1C

Bản thiết kế cần mô tả cấu trúc TOE với các hệ thống con.

11.6.8.2.2 ADV_TDS.5.2C

Bản thiết kế cần mô tả TSF với các mô đun, thiết kế mỗi mô đun theo "bắt buộc theo SFR", "hỗ trợ SFR", hoặc "không liên quan SFR".

11.6.8.2.3 ADV_TDS.5.3C

Bản thiết kế cần chỉ ra tất cả các hệ thống con của TSF.

11.6.8.2.4 ADV_TDS.5.4C

Bản thiết kế cần đưa ra mô tả bán chính thức cho mỗi hệ thống con của TSF, với văn bản giải thích không chính thức phù hợp.

11.6.8.2.5 ADV_TDS.5.5C

Bản thiết kế cần đưa ra mô tả cho các tương tác của mọi hệ thống con của TSF.

11.6.8.2.6 ADV_TDS.5.6C

Bản thiết kế cần đưa ra ánh xạ từ các hệ thống con của TSF đến các mô đun của TSF.

11.6.8.2.7 ADV_TDS.5.7C

Bản thiết kế cần mô tả **bán chính thức** mỗi mô đun với **mục đích, tương tác, giao diện** của chúng, cho lại các giá trị từ các giao diện này, tương tác với và gọi các giao diện tới các mô đun khác, **với văn bản giải thích không chính thức phù hợp**.

11.6.8.2.8 ADV_TDS.5.8C

Bản thiết kế cần biểu thị rằng mọi hoạt động mô tả trong thiết kế TOE được ánh xạ vào trong các TSFI thực thi chúng.

11.6.8.3 Các phần từ hành động của đánh giá viên

11.6.8.3.1 ADV_TDS.5.1E

Đánh giá viên cần khẳng định rằng thông tin đã cung cấp đáp ứng mọi yêu cầu về nội dung và biểu thị bằng chứng.

11.6.8.3.2 ADV_TDS.5.2E

Đánh giá viên cần xác định rằng bản thiết kế là một bản sao chính xác và đầy đủ mọi yêu cầu chức năng an toàn.

11.6.9 ADV_TDS.6 Thiết kế mô đun bán chính thức đầy đủ với bản thể hiện thiết kế chính thức mức cao

Các phụ thuộc: ADV_FSP.6 Đặc tả chức năng bán chính thức đầy đủ với bổ sung đặc tả chính thức

11.6.9.1 Phần từ hành động của nhà phát triển

11.6.9.1.1 ADV_TDS.6.1D

Nhà phát triển cần đưa ra được bản thiết kế của TOE.

11.6.9.1.2 ADV_TDS.6.2D

Nhà phát triển cần đưa ra được bản ánh xạ giữa TSFI về đặc tả chức năng và mức phân tách thấp nhất dùng được trong thiết kế TOE.

11.6.9.1.3 ADV_TDS.6.3D

Nhà phát triển cần đưa ra được đặc tả chính thức cho các hệ thống con TSF.

11.6.9.1.4 ADV_TDS.6.4D

Nhà phát triển cần đưa ra được minh chứng về sự phù hợp giữa các đặc tả chính thức cho các hệ thống con TSF và cho đặc tả chức năng.

11.6.9.2 Các phần từ nội dung và trình bày

11.6.9.2.1 ADV_TDS.6.1C

Bản thiết kế cần mô tả cấu trúc TOE với các hệ thống con.

11.6.9.2.2 ADV_TDS.6.2C

Bản thiết kế cần mô tả TSF với các mô đun, thiết kế mỗi mô đun theo "bắt buộc theo SFR", "hỗ trợ SFR", hoặc "không liên quan SFR".

11.6.9.2.3 ADV_TDS.6.3C

Bản thiết kế cần chỉ ra tất cả các hệ thống con của TSF.

11.6.9.2.4 ADV_TDS.6.4C

Bản thiết kế cần đưa ra mô tả bán chính thức cho mỗi hệ thống con của TSF, với văn bản giải thích không chính thức phù hợp.

11.6.9.2.5 ADV_TDS.6.5C

Bản thiết kế cần đưa ra mô tả cho các tương tác của mọi hệ thống con của TSF.

11.6.9.2.6 ADV_TDS.6.6C

Bản thiết kế cần đưa ra ánh xạ từ các hệ thống con của TSF đến các mô đun của TSF.

11.6.9.2.7 ADV_TDS.6.7C

Bản thiết kế cần mô tả **theo kiểu bán chính thức** cho mỗi mô đun với mục đích, tương tác, các giá trị cho lại từ các giao diện này, và các giao diện được gọi tới các mô đun khác, với văn bản giải thích không chính thức phù hợp.

11.6.9.2.8 ADV_TDS.6.8C

Đặc tả chính thức của các hệ thống con TSF cần mô tả TSF theo kiểu chính thức, kèm văn bản giải thích không chính thức phù hợp.

11.6.9.2.9 ADV_TDS.6.9C

Ánh xạ cần biểu thị rằng mọi hoạt động mô tả trong thiết kế TOE được ánh xạ vào trong các TSFI thực thi chúng.

11.6.9.2.10 ADV_TDS.6.10C

Minh chứng cho sự phù hợp giữa các đặc tả chính thức cho các hệ thống con TSF và cho đặc tả chức năng cần biểu thị rằng mọi hoạt động mô tả trong thiết kế TOE là bản chi tiết hóa một cách đầy đủ và chính xác của TSFI thực thi chúng.

11.6.9.3 Các phần tử hành động của đánh giá viên

11.6.9.3.1 ADV_TDS.6.1E

Đánh giá viên cần khẳng định rằng thông tin đã cung cấp đáp ứng mọi yêu cầu về nội dung và biểu thị bằng chứng.

11.6.9.3.2 ADV_TDS.6.2E

Đánh giá viên cần xác định rằng bản thiết kế là một bản sao chính xác và đầy đủ mọi yêu cầu chức năng an toàn.

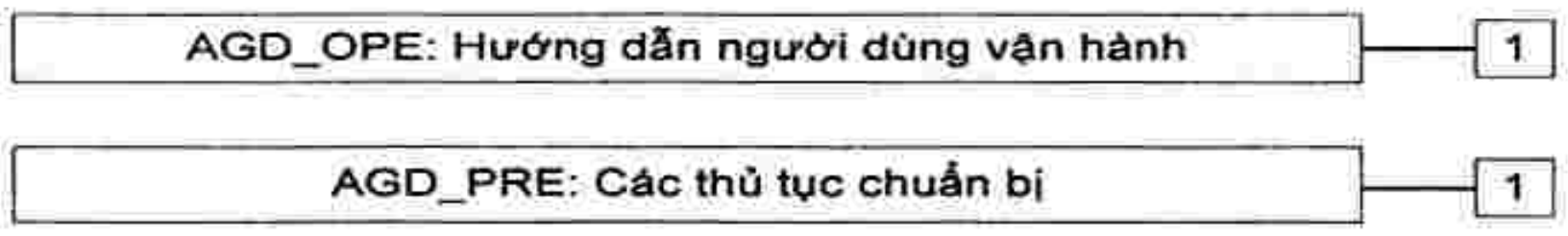
12 Lớp AGD: Tài liệu hướng dẫn

Lớp tài liệu hướng dẫn đưa ra những yêu cầu cho tài liệu hướng dẫn cho người sử dụng. Đối với việc chuẩn bị và vận hành an toàn TOE, điều này là cần thiết để mô tả tất cả những vấn đề về xử lý an toàn của TOE. Lớp cũng đề cập đến khả năng cấu hình không đúng như mong muốn hoặc việc xử lý TOE.

Trong nhiều trường hợp, có thể thích hợp hơn là hướng dẫn được chia ra nhiều tài liệu cho chuẩn bị và vận hành an toàn TOE, hoặc các tài liệu riêng cho những người sử dụng khác nhau như: người dùng đầu cuối, quản trị viên, người lập trình ứng dụng sử dụng các giao diện phần cứng, phần mềm...

Lớp tài liệu hướng dẫn được chia thành hai họ, có liên quan đến phần hướng dẫn chuẩn bị cho người dùng (là điều cần thực hiện khi chuyển đổi TOE đã bàn giao sang cấu hình đã đánh giá trong môi trường vận hành như đã mô tả trong ST) và với phần hướng dẫn người dùng vận hành (những gì cần thực hiện trong quá trình khai thác TOE trong cấu hình đã đánh giá của nó.

Hình 12 biểu thị các họ trong lớp này, phân lớp thành phần trong các họ.



Hình 12 - Phân cấp lớp AGC: Các tài liệu hướng dẫn

12.1 Hướng dẫn người dùng vận hành (AGD_OPE)

12.1.1 Mục tiêu

Tài liệu hướng dẫn này đề cập đến các tài liệu văn bản dành cho những người dùng TOE trong cấu hình đã đánh giá của nó bao gồm: người dùng đầu cuối, người có trách nhiệm duy trì và quản lý TOE theo cách đúng nhằm đạt sự an toàn tối đa, và những người dùng khác (ví dụ các lập trình viên) sử dụng các giao diện TOE với bên ngoài. Tài liệu hướng dẫn người dùng vận hành mô tả chức năng an toàn cung cấp bởi TSF, đưa ra các lệnh và hướng dẫn (gồm cả cảnh báo), giúp hiểu được TSF và bao gồm thông tin an toàn trọng yếu, các hành động an toàn trọng yếu cần có, nhằm đảm bảo sử dụng chúng an toàn. Hướng dẫn sai hoặc không hợp lý cần loại bỏ khỏi tài liệu hướng dẫn, các thủ tục an toàn cho mọi chế độ hoạt động cần được xem xét. Các trạng thái không an toàn cần dễ phát hiện.

Hướng dẫn người dùng vận hành đưa ra biện pháp tin cậy giúp các người sử dụng thông thường, các quản trị viên, các nhà cung cấp ứng dụng và những đối tượng khác liên quan đến giao diện bên ngoài TOE hiểu được hoạt động an toàn của TOE và sử dụng nó như đã dự kiến. Đánh giá hướng dẫn người dùng bao gồm cả việc xem xét xem TOE có thể sử dụng theo cách không an toàn như thế nào và người dùng TOE cẫn tin là nó hoạt động an toàn. Mục tiêu là giảm thiểu rủi do do con người và các lỗi khác khi hoạt động có thể gây ra ngăn cản, làm sai hoặc chặn chức năng an toàn để đưa TOE vào trạng thái không an toàn không thể phát hiện được.

12.1.2 Phân mức thành phần

Họ này chỉ gồm một thành phần.

12.1.3 Chú thích ứng dụng

Có thể các vai trò người dùng và nhóm người dùng khác nhau được chấp thuận trong TOE và họ có thể tương tác với TSF. Vai trò người dùng và các nhóm này cần được xem xét trong tài liệu hướng dẫn người dùng vận hành. Họ có thể được nhóm vào quản trị viên và những người dùng không có vai trò quản trị, hoặc cụ thể hơn được nhóm vào các cá nhân có trách nhiệm về việc: nhận, chấp thuận, cài

đặt và duy trì TOE, lập trình viên các ứng dụng, người soát xét, kiểm toán viên, quản trị viên hàng ngày, người dùng đầu cuối. Mỗi vai trò có thể bao hàm một tập năng lực hoặc chỉ một quyền duy nhất.

Yêu cầu AGD_OPE.1.1C bao hàm khía cạnh mọi cảnh báo tới người dùng trong khi vận hành TOE sẽ liên quan đến định nghĩa vấn đề an toàn và các mục tiêu an toàn cho môi trường vận hành được mô tả trong PP/ST là phù hợp trong hướng dẫn người dùng.

Khái niệm các giá trị an toàn, như đã nêu trong AGD_OPE.1.3.C có liên quan về vị trí người dùng có quyền kiểm soát các tham số an toàn. Hướng dẫn cần đưa ra đối với việc đặt đúng và không an toàn các tham số trên.

AGD_OPE.1.4C đòi hỏi hướng dẫn người dùng phải mô tả các phản ứng phù hợp với các sự kiện an toàn liên quan. Mặc dù nhiều sự kiện an toàn là kết quả của thực hiện các chức năng, cũng không nhất thiết phải như vậy trong một số trường hợp (ví dụ kiểm toán bản ghi nhật ký, phát hiện một xâm nhập). Ngoài ra, một sự kiện liên quan an toàn có thể xảy ra là kết quả của một chuỗi ácc chức năng, hoặc, ngược lại, một số sự kiện an toàn có thể xảy ra với một chức năng.

AGD_OPE.1.7C đòi hỏi rằng hướng dẫn người dùng phải rõ ràng và hợp lý. Hướng dẫn sai hoặc không hợp lý có thể dẫn đến việc một người dùng TOE tin rằng TOE an toàn trong khi nó không phải như vậy.

Một ví dụ về hướng dẫn sai có thể là mô tả về một lệnh hướng dẫn đơn lẻ có thể truyền theo nhiều cách, một trong những cách đó có thể dẫn đến trạng thái không an toàn.

Một ví dụ về hướng dẫn không an toàn có thể là một khuyến nghị tuân theo một thủ tục mà nó quá phức tạp không thể kỳ vọng như mong muốn là người dùng thực hiện theo.

12.1.4 Hướng dẫn người dùng vận hành AGD_OPE.1

Phụ thuộc: ADV_FSP.1 Đặc tả chức năng cơ bản

12.1.4.1 Các thành phần hành động nhà phát triển

12.1.4.1.1 AGD_OPE.1.1D

Nhà phát triển cần đưa ra tài liệu hướng dẫn người dùng vận hành.

12.1.4.2 Các phần tử nội dung và trình bày

12.1.4.2.1 AGD_OPE.1.1C

Tài liệu hướng dẫn người dùng vận hành cần mô tả các vai trò từng người, các chức năng truy nhập người dùng và các đặc quyền cần được kiểm soát trong môi trường xử lý an toàn, bao gồm các cảnh báo phù hợp.

12.1.4.2.2 AGD _OPE.1.2C

Tài liệu hướng dẫn người dùng vận hành cần mô tả các vai trò từng người, cách thức sử dụng các giao diện sẵn có cung cấp bởi TOE theo cách an toàn.

12.1.4.2.3 AGD_OPE.1.3C

Tài liệu hướng dẫn người dùng vận hành cần mô tả các vai trò từng người, các chức năng sẵn có và các giao diện, cụ thể là mọi tham số an toàn dưới sự kiểm soát của người dùng, biểu thị các giá trị an toàn phù hợp.

12.1.4.2.4 AGD _OPE.1.4C

Tài liệu hướng dẫn người dùng vận hành cần mô tả các vai trò từng người, định rõ mỗi kiểu sự kiện an toàn liên quan tương đối so với các chức năng truy nhập người dùng cần thực hiện, bao gồm việc thay đổi các đặc tính an toàn của các thực thể dưới sự kiểm soát của TSF.

12.1.4.2.5 AGD _OPE.1.5C

Tài liệu hướng dẫn người dùng vận hành cần xác định mọi chế độ hoạt động có thể của TOE (bao gồm hoạt động sau lỗi và lỗi vận hành), tính hợp lý của chúng và các ngầm định nhằm duy trì hoạt động an toàn.

12.1.4.2.6 AGD_OPE.1.6C

Tài liệu hướng dẫn người dùng vận hành cần mô tả cho vai trò từng người, các biện pháp an toàn cần theo nhằm thỏa mãn các mục tiêu an toàn cho môi trường hoạt động như đã mô tả trong ST.

12.1.4.2.7 AGD_OPE.1.7C

Tài liệu hướng dẫn người dùng vận hành cần rõ ràng và hợp lý.

12.1.4.3 Các phần tử hành động của đánh giá viên

12.1.4.3.1 AGD_OPE.1.1E

Đánh giá viên cần xác nhận thông tin đưa ra đáp ứng mọi nhu cầu về nội dung và trình bày của chứng cứ.

12.2 Các thủ tục chuẩn bị (AGD_PRE)

12.2.1 Mục tiêu

Các thủ tục chuẩn bị dùng để đảm bảo rằng TOE đã được nhận, cài đặt theo cách an toàn như dự kiến bởi nhà phát triển. Các yêu cầu chuẩn bị đặt ra nhiệm vụ chuyển đổi an toàn từ TOE đã bàn giao sang môi trường vận hành ban đầu của nó. Điều này bao gồm việc xem xét xem TOE có thể được cấu hình hoặc cài đặt theo cách không an toàn mà người dùng TOE vẫn tin rằng nó an toàn hay không.

12.2.2 Phân mức thành phần

Họ này chỉ gồm một thành phần

12.2.3 Chú thích ứng dụng

Có thể thấy áp dụng các yêu cầu này sẽ khác nhau tùy theo góc độ TOE có được chuyển giao vào trạng thái vận hành hay không, hay nó được cài đặt tại địa điểm của chủ sở hữu TOE,...

Quy trình đầu tiên liên quan các thủ tục chuẩn bị là việc chấp nhận an toàn của người tiêu dùng khi nhận TOE tuân theo các thủ tục chuyển giao từ nhà phát triển. Nếu nhà phát triển không định nghĩa các thủ tục chuyển giao, thì an toàn cho việc chấp nhận cũng cần đảm bảo.

Việc cài đặt TOE bao gồm chuyển đổi môi trường vận hành của nó vào trạng thái tuân thủ theo các mục tiêu an toàn cho môi trường vận hành đã đưa ra trong ST.

Có thể có trường hợp không cần thiết phải cài ddawth, ví dụ một thẻ thông minh. Trong trường hợp này, có thể không phù hợp nếu yêu cầu và phân tích các thủ tục cài đặt.

Các yêu cầu trong họ bảo đảm này được trình bày tách biệt với họ Hướng dẫn người dùng vận hành (AGD_OPE), bởi vì việc sử dụng không thường xuyên và chỉ một lần của các thủ tục chuẩn bị.

12.2.4 Các thủ tục chuẩn bị AGD_PRE.1

Các mối phụ thuộc: không có sự phụ thuộc nào.

12.2.4.1 Phần tử hành động của nhà phát triển

12.2.4.1.1 AGD_PRE.1.1D

Nhà phát triển cần cung cấp TOE bao gồm các thủ tục chuẩn bị nó.

12.2.4.2 Các phần tử nội dung và trình bày

12.2.4.2.1 AGD_PRE.1.1C

Các thủ tục chuẩn bị cần mô tả mọi bước cần thiết để chấp nhận an toàn cho TOE đã chuyển giao tuân theo các thủ tục chuyển giao của nhà phát triển.

12.2.4.2.2 AGD_PRE.1.2C

Các thủ tục chuẩn bị cần mô tả mọi bước cần thiết cho cài đặt an toàn TOE và chuẩn bị an toàn môi trường vận hành tuân theo các mục tiêu an toàn cho môi trường vận hành đã mô tả trong ST.

12.2.4.3 Các phần tử hành động của đánh giá viên

12.2.4.3.1 AGD_PRE.1.1E

Đánh giá viên cần xác nhận thông tin cung cấp đáp ứng mọi nhu cầu về nội dung và trình bày của chứng cứ.

12.2.4.3.2 AGD_PRE.1.2E

Đánh giá viên cần áp dụng các thủ tục chuẩn bị để khẳng định rằng TOE cần được chuẩn bị an toàn cho hoạt động.

13 Lớp ALC: Hỗ trợ vòng đời

Hỗ trợ vòng đời là một khía cạnh của tạo lập qui tắc và kiểm soát trong quá trình bổ sung chi tiết của TOE trong khi phát triển và duy trì nó. Tính tin cậy trong trao đổi giữa các yêu cầu an toàn TOE và TOE là lớn hơn nếu phân tích an toàn và việc đưa ra chứng cớ được làm trên cơ sở điều tiết như một phần toàn vẹn của các hoạt động phát triển và duy trì.

Trong vòng đời sản phẩm, việc phân biệt xem TOE là trách nhiệm của nhà phát triển hay người dùng được quan tâm hơn là nó thuộc môi trường phát triển hay môi trường người dùng. Ranh giới chuyển đổi là thời điểm bàn giao TOE cho người dùng. Đó cũng là thời điểm chuyển đổi từ lớp ALC sang lớp AGD.

Lớp ALC bao gồm 7 họ. Họ Định nghĩa vòng đời (ALC_LCD) mô tả mức cao cho vòng đời TOE. Họ Năng lực CM (ALC_CM) mô tả chi tiết hơn về việc quản lý các danh mục lập cấu hình. Phạm vi CM (ALC_CMS) đòi hỏi một tập danh mục cấu hình tối thiểu cần quản lý theo cách đã xác định. An toàn phát triển (ALC_DVS) liên quan đến các biện pháp về vật lý, thủ tục và con người cũng như các biện pháp an toàn khác của nhà phát triển. Công cụ và kỹ thuật (ALC_TAT) liên quan đến các công cụ phát triển và tiêu chuẩn triển khai do nhà phát triển sử dụng. Sửa lỗi (ALC_FLR) liên quan đến việc xử lý các khiếm khuyết về an toàn. Chuyển giao (ALC_DEL) định nghĩa các thủ tục dùng cho chuyển giao TOE tới khách hàng. Các quy trình chuyển giao xuất hiện trong phát triển TOE nặng về nghĩa vận

chuyển, chúng được sử dụng trong ngữ cảnh các thủ tục tích hợp và chấp nhận trong các họ khác của lớp này.

Trong toàn bộ lớp này, phát triển và các thuật ngữ liên quan (nhà phát triển, động từ phát triển) được hiểu với nghĩa rộng hơn bao gồm phát triển và *sản xuất*, trong đó sản xuất có nghĩa đặc biệt là quy trình chuyển đổi biểu diễn triển khai sang TOE thành phẩm.

Hình 13 cho thấy các họ trong lớp này, và phân cấp các thành phần trong các họ.

Hình 13 - Phân cấp lớp ALC: Hỗ trợ vòng đời

13.1 Năng lực CM (ALC_CMC)

13.1.1 Mục tiêu

Quản lý cấu hình (CM) là cách để tăng thêm tính đảm bảo về việc TOE thỏa mãn các SFRs. CM tạo ra điều đó bằng cách yêu cầu nguyên tắc và biện pháp quản lý trong các quy trình cụ thể hóa và sửa đổi TOE và thông tin liên quan. Các hệ thống CM được đưa ra nhằm đảm bảo tính toàn vẹn cho các phần của TOE mà chúng kiểm soát, bằng cách đưa ra phương pháp theo dấu các thay đổi và qua việc đảm bảo rằng mọi thay đổi đều được phép.

Mục tiêu của họ này là yêu cầu hệ thống CM của nhà phát triển có một số năng lực nhất định. Nghĩa là có thể giảm khả năng xảy ra việc sửa đổi ngẫu nhiên hoặc trái phép các danh mục trong cấu hình. Hệ thống CM cần đảm bảo tính toàn vẹn của TOE từ khâu thiết kế ban đầu trong suốt quá trình duy trì hoạt động sau đó.

Mục tiêu của việc đưa vào các công cụ CM tự động hóa là làm tăng tính hiệu quả của hệ thống CM. Trong khi các hệ thống CM tự động và thủ công có thể bị vượt qua, bỏ qua hoặc chứng tỏ là không đủ để phòng chống các sửa đổi trái phép, các hệ thống tự động hóa ít chịu ảnh hưởng hơn bởi lỗi của con người hoặc những sơ xuất.

Mục đích của họ này bao gồm:

a) Đảm bảo rằng TOE là chính xác và toàn vẹn trước khi được gửi tới khách hàng.

b) Đảm bảo không có danh mục cấu hình bị thiếu trong quá trình đánh giá

c) Chống lại sự thay đổi, thêm vào, hay xoá trái phép các danh mục cấu hình TOE.

13.1.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở năng lực hệ thống CM, phạm vi của tài liệu CM và chứng cứ cung cấp bởi nhà phát triển.

13.1.3 Chú thích ứng dụng

Mặc dù mong muốn CM được áp dụng ngay từ khâu thiết kế ban đầu và tiếp tục sau đó, họ này đòi hỏi CM cần được đặt ra và sử dụng trước khi kết thúc đánh giá.

Trong trường hợp TOE là một phần nhỏ của sản phẩm, các yêu cầu của họ này chỉ áp dụng cho danh mục cấu hình TOE mà không cho toàn bộ sản phẩm.

Đối với nhà phát triển có các hệ thống CM riêng cho các chu trình vòng đời khác nhau (ví dụ phát triển, sản xuất và/hoặc sản phẩm cuối), cần văn bản hóa mọi quá trình này. Cho các mục đích đánh giá, các hệ thống CM riêng biệt cần được xem như các phần của một hệ thống CM tổng quát được đề cập trong các tiêu chí.

Tương tự, nếu các phần của TOE được tạo ra bởi các nhà phát triển khác nhau ở các nơi khác nhau, các hệ thống CM đang sử dụng ở các địa điểm khác nhau cần được xem như các phần của một hệ thống CM tổng quát được đề cập trong các tiêu chí. Trong tình huống này, cần xem xét thêm các vấn đề tích hợp.

Một số phần tử của họ này tham chiếu tới danh mục cấu hình. Các phần tử này xác định các yêu cầu CM cần được áp đặt vào mọi mục đã nêu trong danh sách cấu hình, song nội dung cụ thể của danh sách sẽ là phần việc của nhà phát triển. Phạm vi CM (ALC_CMS) có thể dùng để hạn chế việc cụ thể hóa này bằng việc xác định ra các mục đặc trưng cần phải có trong danh sách cấu hình, nghĩa là có trong CM.

ALC_CMC.2.3C đưa ra một yêu cầu về việc hệ thống CM định danh thống nhất mọi danh mục cấu hình. Điều này cũng đòi hỏi các sửa đổi danh mục cấu hình mang lại một định danh mới, duy nhất được gán cho danh mục cấu hình.

ACM_CAP.3.8C đưa ra một yêu cầu là cần có bằng chứng thể hiện rằng hệ thống CM hoạt động tuân theo kế hoạch CM. Ví dụ các bằng chứng có thể là tài liệu như là bản chụp màn hình hoặc kết quả vết kiểm toán đưa ra từ hệ thống CM, hoặc một công bố chi tiết về hệ thống CM bởi nhà phát triển. Đánh giá viên có trách nhiệm xác định bằng chứng nào là đủ để chỉ ra rằng hệ thống CM hoạt động tuân theo kế hoạch CM.

ALC_CMC4.5C đưa ra một yêu cầu là hệ thống CM cung cấp một phương pháp tự động để hỗ trợ sản xuất TOE. Điều này đòi hỏi hệ thống CM cung cấp một phương pháp hỗ trợ việc xác định rằng danh mục cấu hình chính xác đã được sử dụng để tạo ra TOE.

ALC_CMC5.10C đưa ra một yêu cầu là hệ thống CM cung cấp một phương pháp tự động để xác nhận những thay đổi của TOE và phiên bản trước đó. Nếu không có phiên bản trước đó của TOE, nhà phát triển vẫn cần cung cấp một phương pháp để xác nhận sự thay đổi của TOE và phiên bản tương lai.

13.1.4 ALC_CMC.1 Gán nhãn TOE

Các mối phụ thuộc: ALC_CMS.1 TOE CM Tổng quát

13.1.4.1 Mục tiêu

Một tham chiếu duy nhất được yêu cầu để đảm bảo rằng không có sự mơ hồ về trường hợp TOE được đánh giá. Gán nhãn TOE với tham chiếu đó đảm bảo rằng người sử dụng TOE có thể nhận thức được tình huống TOE nào thì họ sử dụng.

13.1.4.2 Các thành phần hành động nhà phát triển

13.1.4.2.1 ALC_CMC.1.1D

Nhà phát triển cần cung cấp TOE và một tham chiếu đến TOE.

13.1.4.3 Các phần tử nội dung và trình bày

13.1.4.3.1 ALC_CMC.1.1C

TOE cần được gán nhãn bằng tham chiếu duy nhất của nó.

13.1.4.4 Các phần tử hành động của đánh giá viên

13.1.4.4.1 ALC_CMC.1.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và thể hiện của chứng cứ.

13.1.5 ALC_CMC.2 Sử dụng hệ thống CM

Các mối phụ thuộc: ALC_CMS.1 TOE CM Tổng quát

13.1.5.1 Mục tiêu

Một tham chiếu duy nhất được yêu cầu để đảm bảo rằng không có sự mơ hồ về bản TOE đang được đánh giá. Gán nhãn TOE với tham chiếu đó đảm bảo rằng người sử dụng TOE có thể nhận thức được bản TOE nào họ đang sử dụng.

Định danh duy nhất của danh mục cấu hình dẫn đến việc hiểu rõ ràng về việc tổng hợp TOE, từ đó giúp xác định các mục nào cần đối với các yêu cầu đánh giá TOE.

Việc sử dụng một hệ thống CM làm tăng tính bảo đảm rằng danh mục cấu hình đang được duy trì có kiểm soát.

13.1.5.2 Phần tử hành động của nhà phát triển

13.1.5.2.1 ALC_CMC.2.1D

Nhà phát triển cần cung cấp TOE và một tham chiếu đến TOE.

13.1.5.2.2 ALC_CMC2.2D

Nhà phát triển cần cung cấp tài liệu CM

13.1.5.2.3 ALC_CMC2.3D

Nhà phát triển cần sử dụng một hệ thống CM

13.1.5.3 Các phần tử nội dung và trình bày

13.1.5.3.1 ALC_CMC2.1C

TOE cần gán nhãn với tham chiếu duy nhất của nó.

13.1.5.3.2 ALC_CMC2.2C

Tài liệu CM cần miêu tả phương thức sử dụng để xác định một cách duy nhất danh mục cấu hình.

13.1.5.3.3 ALC_CMC2.3C

Hệ thống CM cần xác định một cách duy nhất tất cả các mục cấu hình.

13.1.5.4 Các phần tử hành động của đánh giá viên

13.1.5.4.1 ACM_CMC.2.1E

Đánh giá viên cần xác nhận rằng thông tin được đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.1.6 ALC_CMC.3 Kiểm soát cấp phép

Các mối phụ thuộc: ALC_CMS.1 TOE CM Tổng quát

ALC_DVS.1 xác định các biện pháp an toàn

ALC_LCD.1 mô hình vòng đời xác định bởi nhà phát triển

13.1.6.1 Mục tiêu

Một tham chiếu duy nhất được yêu cầu để đảm bảo rằng không có sự mơ hồ về trường hợp TOE được đánh giá. Gán nhãn TOE với tham chiếu đó đảm bảo rằng người sử dụng TOE có thể nhận thức được tình huống TOE nào thì họ sử dụng.

Sự xác định duy nhất của danh mục cấu hình hướng dẫn để hiểu rõ hơn cấu trúc TOE, nó giúp xác định danh mục nào là chính đối với các yêu cầu đánh giá cho TOE.

Việc sử dụng một hệ thống CM làm tăng tính bảo đảm rằng danh mục cấu hình đang được duy trì có kiểm soát.

Cung cấp kiểm soát để đảm bảo rằng các thay đổi trái phép không xảy ra trong TOE ("kiểm soát truy nhập CM"), đảm bảo chức năng thích hợp và sử dụng của hệ thống CM, giúp để duy trì tính toàn vẹn trong TOE.

13.1.6.2 Phần tử hành động của nhà phát triển

13.1.6.2.1 ACM_CMC.3.1D

Nhà phát triển cần cung cấp TOE và một tham chiếu đến TOE.

13.1.6.2.2 ACM_CMC.3.2D

Nhà phát triển cần cung cấp tài liệu CM

13.1.6.2.3 ACM_CMC.3.3D

Nhà phát triển cần sử dụng hệ thống CM.

13.1.6.3 Các phần tử nội dung và trình bày

13.1.6.3.1 ACM_CMC.3.1C

TOE cần được gán nhãn với tham chiếu duy nhất của nó.

13.1.6.3.2 ACM_CMC.3.2C

Tài liệu CM cần miêu tả phương thức sử dụng để xác định một cách duy nhất danh mục cấu hình.

13.1.6.3.3 ACM_CMC.3.3C

Hệ thống CM cần xác định một cách duy nhất tất cả các mục cấu hình.

13.1.6.3.4 ACM_CMC.3.4C

Hệ thống CM cần cung cấp các biện pháp như chỉ các thay đổi hợp lệ mới được chấp nhận cho các mục cấu hình.

13.1.6.3.5 ACM_CMC.3.5C

Tài liệu CM cần bao gồm kế hoạch CM.

13.1.6.3.6 ACM_CMC.3.6C

Kế hoạch CM cần mô tả hệ thống CM được dùng để phát triển TOE như thế nào.

13.1.6.3.7 ACM_CMC.3.7C

Bằng chứng cần chứng tỏ rằng tất cả các mục cấu hình đang được duy trì bởi hệ thống CM.

13.1.6.3.8 ACM_CMC.3.8C

Bằng chứng cần chứng tỏ rằng hệ thống CM đang hoạt động theo kế hoạch CM.

13.1.6.4 Các phần tử hành động của đánh giá viên

13.1.6.4.1 ACM_CMC.3.1E

Đánh giá viên cần xác nhận rằng thông tin được đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.1.7 ACM_CMC.4 Hỗ trợ sản xuất và các thủ tục chấp nhận và tự động hóa

Các mối phụ thuộc: ALC_CMS.1 TOE CM Tổng quát

ALC_DVS.1 xác định các biện pháp an toàn

ALC_LCD.1 mô hình vòng đời xác định bởi nhà phát triển

13.1.7.1 Mục tiêu

Một tham chiếu duy nhất được yêu cầu để đảm bảo rằng không có sự mơ hồ về trường hợp TOE được đánh giá. Gán nhãn TOE với tham chiếu đó đảm bảo rằng người sử dụng TOE có thể nhận thức được tình huống TOE nào thì họ sử dụng.

Sự xác định duy nhất của danh mục cấu hình hướng dẫn để hiểu rõ hơn cấu trúc TOE, nó giúp xác định danh mục nào là chính đối với các yêu cầu đánh giá cho TOE.

Sử dụng hệ thống CM tăng cường đảm bảo rằng các danh mục cấu hình được duy trì một cách có kiểm soát.

Cung cấp kiểm soát để đảm bảo rằng các thay đổi trái phép không xảy ra trong TOE ("kiểm soát truy nhập CM"), và đảm bảo chức năng thích hợp và sử dụng của hệ thống CM, giúp để duy trì tính toàn vẹn trong TOE.

Mục đích của các thủ tục chấp nhận là đảm bảo rằng các phần của TOE có chất lượng phù hợp và khẳng định rằng mọi sự tạo mới hoặc sửa đổi danh mục cấu hình là được phép. Các thủ tục chấp nhận là một phần tử quan trong trong các quy trình tích hợp và trong quản lý vòng đời của TOE.

Trong các môi trường phát triển với danh mục cấu hình phức tạp, rất khó có thể kiểm soát thay đổi mà không có sự hỗ trợ của các công cụ tự động hóa. Cụ thể là các công cụ tự động hóa này cần thiết để có thể hỗ trợ một số lớn các thay đổi xuất hiện trong phát triển và đảm bảo rằng các thay đổi đó là được phép. Một mục tiêu của thành phần này là đảm bảo rằng danh mục cấu hình được kiểm soát thông qua phương pháp tự động hóa. Nếu TOE được phát triển bởi nhiều nhà phát triển, nghĩa là có sự tích hợp, sử dụng công cụ tự động hóa là điều hợp lý.

Các thủ tục hỗ trợ sản xuất giúp đảm bảo rằng việc sinh ra TOE từ một tập danh mục cấu hình có kiểm soát được thực hiện chính xác theo phương thức được phép, cụ thể là trong trường hợp khi có nhiều nhà phát triển khác nhau liên quan và các quy trình tích hợp khác nhau cần thực hiện.

13.1.7.2 Phần tử hành động của nhà phát triển

13.1.7.2.1 ACM_CMC.4.1D

Nhà phát triển cần cung cấp TOE và một tham chiếu đến TOE.

13.1.7.2.2 ACM_CMC.4.2D

Nhà phát triển cần cung cấp tài liệu CM.

13.1.7.2.3 ACM_CMC.4.3D

Nhà phát triển cần sử dụng một hệ thống CM.

13.1.7.3 Các phần tử nội dung và trình bày

13.1.7.3.1 ALC_CMC.4.1C

TOE cần được gán nhãn với tham chiếu duy nhất của nó.

13.1.7.3.2 ALC_CMC.4.2C

Tài liệu CM cần miêu tả phương thức sử dụng để xác định một cách duy nhất danh mục cấu hình.

13.1.7.3.3 ALC_CMC.4.3C

Hệ thông CM cần xác định một cách duy nhất tất cả các mục cấu hình.

13.1.7.3.4 ALC_CMC.4.4C

Hệ thống CM cần cung cấp các biện pháp **tự động hóa** để chỉ các thay đổi hợp lệ mới được chấp nhận đối với các mục cấu hình.

13.1.7.3.5 ALC_CMC.4.5C

Hệ thống CM cần hỗ trợ sự sản xuất TOE bằng phương thức tự động.

13.1.7.3.6 ALC_CMC.4.6C

Tài liệu CM cần bao gồm kế hoạch CM.

13.1.7.3.7 ALC_CMC.4.7C

Kế hoạch CM cần mô tả hệ thống CM được dùng để phát triển TOE như thế nào.

13.1.7.3.8 ALC_CMC.4.8C

Kế hoạch CM cần mô tả các thủ tục sử dụng để chấp nhận các thay đổi hoặc các mục cấu hình được tạo mới như là một phần của TOE.

13.1.7.3.9 ALC_CMC.4.9C

Bằng chứng cần chứng tỏ rằng tất cả các mục cấu hình đang được duy trì dưới hệ thống CM.

13.1.7.3.10 ALC_CMC.4.10C

Bằng chứng cần chứng tỏ rằng hệ thống CM đang được hoạt động phù hợp với kế hoạch CM.

13.1.7.4 Các phần tử hành động của đánh giá viên

13.1.7.4.1 ALC_CMC.4.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.1.8 ALC_CMC.5 Hỗ trợ cải tiến

Các mối phụ thuộc: ALC_CMS.1 TOE CM Tổng quát

ALC_DVS.2 Sự đầy đủ của các biện pháp an toàn

ALC_LCD.1 mô hình vòng đời xác định bởi nhà phát triển

13.1.8.1 Mục tiêu

Một tham chiếu duy nhất được yêu cầu để đảm bảo rằng không có sự mơ hồ về trường hợp TOE được đánh giá. Gán nhãn TOE với tham chiếu đó đảm bảo rằng người sử dụng TOE có thể nhận thức được tình huống TOE nào thì họ sử dụng.

Sự xác định duy nhất của danh mục cấu hình hướng dẫn để hiểu rõ hơn cấu trúc TOE, nó giúp xác định danh mục nào là chính đối với các yêu cầu đánh giá cho TOE.

Sử dụng hệ thống CM tăng cường đảm bảo rằng các danh mục cấu hình được duy trì một cách có kiểm soát.

Cung cấp kiểm soát để đảm bảo rằng các thay đổi trái phép không xảy ra trong TOE ("kiểm soát truy nhập CM"), và đảm bảo chức năng thích hợp và sử dụng của hệ thống CM, giúp để duy trì tính toàn vẹn trong TOE.

Mục đích của các thủ tục chấp nhận là đảm bảo rằng các phần của TOE có chất lượng phù hợp và khẳng định rằng mọi sự tạo mới hoặc sửa đổi danh mục cấu hình là được phép. Các thủ tục chấp nhận là một phần tử quan trong trong các quy trình tích hợp và trong quản lý vòng đời của TOE.

Trong các môi trường phát triển với danh mục cấu hình phức tạp, rất khó có thể kiểm soát thay đổi mà không có sự hỗ trợ của các công cụ tự động hóa. Cụ thể là các công cụ tự động hóa này cần thiết để có thể hỗ trợ một số lớn các thay đổi xuất hiện trong phát triển và đảm bảo rằng các thay đổi đó là được phép. Một mục tiêu của thành phần này là đảm bảo rằng danh mục cấu hình được kiểm soát thông qua phương pháp tự động hóa. Nếu TOE được phát triển bởi nhiều nhà phát triển, nghĩa là có sự tích hợp, sử dụng công cụ tự động hóa là điều hợp lý.

Các thủ tục hỗ trợ sản xuất giúp đảm bảo rằng việc sinh ra TOE từ một tập danh mục cấu hình có kiểm soát được thực hiện chính xác theo phương thức được phép, cụ thể là trong trường hợp khi có nhiều nhà phát triển khác nhau liên quan và các quy trình tích hợp khác nhau cần thực hiện.

Yêu cầu là hệ thống CM cần có khả năng xác định phiên bản biểu diễn triển khai để tạo ra TOE. Điều đó sẽ giúp đảm bảo rằng tính toàn vẹn của tài liệu này được bảo vệ phù hợp về mặt kỹ thuật, vật lý và quy trình.

Cung cấp một phương thức tự động hóa để xác nhận các thay đổi phiên bản của TOE, xác định ra các mục cấu hình nào bị ảnh hưởng bởi việc sửa đổi các mục cấu hình khác và hỗ trợ việc xác định ảnh hưởng của thay đổi giữa các phiên bản trước đó của TOE. Từ đó giúp cung cấp thông tin quý giá để xác định xem các thay đổi TOE mang đến cho mọi danh mục cấu hình có đang nhất quán với nhau hay không.

13.1.8.2 Phần tử hành động của nhà phát triển

13.1.8.2.1 ALC_CMC.5.1D

Nhà phát triển cần cung cấp TOE và một tham chiếu đến TOE.

13.1.8.2.2 ALC_CMC.5.2D

Nhà phát triển cần cung cấp tài liệu CM.

13.1.8.2.3 ALC_CMC.5.3D

Nhà phát triển cần sử dụng một hệ thống CM.

13.1.8.3 Các phần tử nội dung và trình bày

13.1.8.3.1 ALC_CMC.5.1C

TOE cần được gán nhãn với tham chiếu duy nhất của nó.

13.1.8.3.2 ALC_CMC.5.2C

Tài liệu CM cần miêu tả phương thức sử dụng để xác định một cách duy nhất danh mục cấu hình.

13.1.8.3.3 ALC_CMC.5.3C

Tài liệu CM cần điều chỉnh để các thủ tục chấp thuận cung cấp một soát xét đầy đủ và thích hợp các thay đổi đối với tất cả các mục cấu hình.

13.1.8.3.4 ALC_CMC.5.4C

Hệ thông CM cần xác định một cách duy nhất tất cả các mục cấu hình.

13.1.8.3.5 ALC_CMC.5.5C

Hệ thống CM cần cung cấp các biện pháp tự động để chỉ các thay đổi hợp lệ mới được chấp nhận đối với các mục cấu hình.

13.1.8.3.6 ALC_CMC.5.6C

Hệ thống CM cần hỗ trợ sản xuất TOE bằng cách tự động.

13.1.8.3.7 ALC_CMC.5.7C

Hệ thống CM cần bảo đảm rằng người chịu trách nhiệm chấp nhận một mục cấu hình vào CM không phải là nhà phát triển nó.

13.1.8.3.8 ALC_CMC.5.8C

Hệ thống CM cần xác thực các mục cấu hình có trong TSF.

13.1.8.3.9 ALC_CMC.5.9C

Hệ thống CM cần hỗ trợ kiểm toán tất cả sự thay đổi TOE theo phương thức tự động hóa, bao gồm người khởi xướng, ngày và thời gian trong vết kiểm toán.

13.1.8.3.10 ALC_CMC.5.10C

Hệ thống CM cần cung cấp một phương thức tự động để xác định mọi mục cấu hình khác bị ảnh hưởng bởi sự thay đổi của một mục cấu hình đã cho.

13.1.8.3.11 ALC_CMC.5.11C

Hệ thống CM cần có khả năng xác định phiên bản biểu diễn triển khai tạo ra TOE.

13.1.8.3.12 ALC_CMC.5.12C

Tài liệu CM cần bao gồm kế hoạch CM.

13.1.8.3.13 ALC_CMC.5.13C

Kế hoạch CM cần mô tả hệ thống CM được dùng để phát triển TOE như thế nào.

13.1.8.3.14 ALC_CMC.5.14C

Kế hoạch CM cần mô tả các thủ tục sử dụng để chấp nhận các thay đổi hoặc các mục cấu hình được tạo mới như là một phần của TOE.

13.1.8.3.15 ALC_CMC.5.15C

Bằng chứng cần chứng tỏ rằng tất cả các mục cấu hình đang được duy trì dưới hệ thống CM.

13.1.8.3.16 ALC_CMC.4.16C

Bằng chứng cần chứng tỏ rằng hệ thống CM đang được hoạt động phù hợp với kế hoạch CM.

13.1.8.4 Các phần tử hành động của đánh giá viên

13.1.8.4.1 ALC_CMC.5.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.1.8.4.2 ALC_CMC.5.2E

Đánh giá viên cần xác định rằng việc áp dụng các thủ tục hỗ trợ sản xuất sẽ tạo ra TOE như đã được nhà phát triển đưa ra cho các hoạt động kiểm thử.

13.2 Phạm vi CM (ALC_CMS)

13.2.1 Mục tiêu

Mục tiêu của họ này là xác định các mục cần đưa vào danh mục cấu hình và vì vậy đưa vào dưới dạng các yêu cầu CM về năng lực CM (ALC_CMC). Áp dụng quản lý cấu hình cho các mục bổ sung này đưa ra sự đảm bảo rằng tính toàn vẹn của TOE được duy trì.

13.2.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở những gì sau đây được yêu cầu đưa vào danh mục cấu hình: TOE và bằng chứng đánh giá đòi hỏi bởi các SA; các phần của TOE; biểu diễn triển khai; các lỗi an toàn; các công cụ phát triển và thông tin liên quan.

13.2.3 Chú thích ứng dụng

Mặc dù phạm vi CM (ALC_CMS) đòi hỏi một danh sách các mục cấu hình và mỗi mục trong danh sách này thuộc CM, năng lực CM (ALC_CMC) dành phần cụ thể hóa nội dung của danh sách cấu hình cho nhà phát triển. Phạm vi CM (ALC_CMS) hạn chế bớt việc cụ thể hóa này bằng việc xác định các mục bắt buộc phải có trong danh sách cấu hình, do vậy có trong các yêu cầu CM về năng lực CM (ALC_CMC).

13.2.4 ALC_CMS.1 TOE CM Tổng quát

Các mối phụ thuộc: Không có các mối phụ thuộc.

13.2.4.1 Mục tiêu

Một hệ thống CM có thể kiểm soát các thay đổi chỉ với các mục đã đưa vào CM (nghĩa là các mục cấu hình đã xác định trong danh sách cấu hình). Việc đặt bản thân TOE và bằng chứng đánh giá yêu cầu bởi các SAR khác trong ST dưới CM đưa ra sự bảo đảm về việc chúng đã được sửa đổi theo phương thức có kiểm soát với việc cấp quyền chính xác.

13.2.4.2 Chú thích ứng dụng

ALC_CMS.1.1C đưa ra yêu cầu về việc bản thân TOE và bằng chứng đánh giá yêu cầu bởi các SAR khác trong ST đã có trong danh sách cấu hình, và do vậy là chủ thể cho các yêu cầu CM về năng lực CM (ALC_CMC).

13.2.4.3 Phần tử hành động của nhà phát triển

13.2.4.3.1 ALC_CMS.1.1D

Nhà phát triển cần cung cấp một danh sách cấu hình cho TOE.

13.2.4.4 Các phần tử nội dung và trình bày

13.2.4.4.1 ALC_CMS.1.1C

Danh sách cấu hình cần chứa thông tin sau: bản thân TOE; bằng chứng đánh giá đòi hỏi bởi các SAR.

13.2.4.4.2 ALC_CMS.1.2C

Danh sách cấu hình cần xác định duy nhất các mục cấu hình.

13.2.4.5 Các phần tử hành động của đánh giá viên

13.2.4.5.1 ALC_CMS.1.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.2.5 ALC_CMS.2 Các phần của TOE CM tổng quát

Các mối phụ thuộc: Không có các mối phụ thuộc.

13.2.5.1 Mục tiêu

Một hệ thống CM có thể kiểm soát các thay đổi chỉ với các mục đã đưa vào CM (nghĩa là các mục cấu hình đã xác định trong danh sách cấu hình). Việc đặt bản thân TOE, các thành phần cấu thành TOE, và bằng chứng đánh giá yêu cầu bởi các SAR dưới CM đưa ra sự bảo đảm về việc chúng đã được sửa đổi theo phương thức có kiểm soát với các quyền hợp thức.

13.2.5.2 Chú thích ứng dụng

ALC_CMS.2.1C đưa ra yêu cầu về các thành phần cấu thành TOE (tất cả các phần được chuyển giao cho khách hàng, ví dụ như các thành phần phần cứng, hoặc các tệp thi hành được) đã được đưa vào danh sách cấu hình, và do vậy là chủ thể cho các yêu cầu CM về năng lực CM (ALC_CMC).

ALC_CMS.2.3.C đưa ra yêu cầu về việc danh sách cấu hình chỉ ra nhà phát triển của mỗi mục cấu hình liên quan đến TSF. Khái niệm "Nhà phát triển" ở đây không có nghĩa là một người cụ thể mà là một tổ chức có trách nhiệm phát triển danh mục cấu hình.

13.2.5.3 Phần tử hành động của nhà phát triển

13.2.5.3.1 ALC_CMS.2.1D

Nhà phát triển cần cung cấp một danh sách cấu hình cho TOE.

13.2.5.4 Các phần tử nội dung và trình bày

13.2.5.4.1 ALC_CMS.2.1C

Danh sách cấu hình cần chứa thông tin sau: bản thân TOE; bằng chứng đánh giá đòi hỏi bởi các SAR, **tất cả các thành phần cấu thành TOE**.

13.2.5.4.2 ALC_CMS.2.2C

Danh sách cấu hình cần xác định duy nhất các mục cấu hình.

13.2.5.4.3 ALC_CMS.2.3C

Đối với mỗi mục cấu hình liên quan TSF, danh sách cấu hình cần chỉ ra nhà phát triển của mục đó.

13.2.5.5 Các phần tử hành động của đánh giá viên

13.2.5.5.1 ALC_CMS.2.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.2.6 ALC_CMS.3 Biểu diễn triển khai CM tổng quát

Các mối phụ thuộc: Không có các mối phụ thuộc.

13.2.6.1 Mục tiêu

Một hệ thống CM có thể kiểm soát các thay đổi chỉ với các mục đã đưa vào CM (nghĩa là các mục cấu hình đã xác định trong danh sách cấu hình). Việc đặt bản thân TOE, các thành phần cấu thành TOE, **biểu diễn triển khai TOE** và bằng chứng đánh giá yêu cầu bởi các SAR dưới CM đưa ra sự bảo đảm về việc chúng đã được sửa đổi theo phương thức có kiểm soát với các quyền hợp thức.

13.2.6.2 Chú thích ứng dụng

ALC_CMS.3.1C đưa ra yêu cầu về việc biểu diễn triển khai TOE đã được đưa vào danh sách cấu hình, và do vậy là chủ thể cho các yêu cầu CM về năng lực CM (ALC_CMC).

13.2.6.3 Phần tử hành động của nhà phát triển

13.2.6.3.1 ALC_CMS.3.1D

Nhà phát triển cần cung cấp một danh sách cấu hình cho TOE.

13.2.6.4 Các phần tử nội dung và trình bày

13.2.6.4.1 ALC_CMS.3.1C

Danh sách cấu hình cần chứa thông tin sau: bản thân TOE; bằng chứng đánh giá đòi hỏi bởi các SAR, tất cả các thành phần cấu thành TOE; **biểu diễn triển khai TOE**.

13.2.6.4.2 ALC_CMS.3.2C

Danh sách cấu hình cần xác định duy nhất các mục cấu hình.

13.2.6.4.3 ALC_CMS.3.3C

Đối với mỗi mục cấu hình liên quan TSF, danh sách cấu hình cần chỉ ra nhà phát triển của mục đó.

13.2.6.5 Các phần tử hành động của đánh giá viên

13.2.6.5.1 ALC_CMS.3.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.2.7 ALC_CMS.4 Theo dấu vấn đề CM tổng quát

Các mối phụ thuộc: Không có các mối phụ thuộc.

13.2.7.1 Mục tiêu

Một hệ thống CM có thể kiểm soát các thay đổi chỉ với các mục đã đưa vào CM (nghĩa là các mục cấu hình đã xác định trong danh sách cấu hình). Việc đặt bản thân TOE, các thành phần cấu thành TOE, và bằng chứng đánh giá yêu cầu bởi các SAR dưới CM đưa ra sự bảo đảm về việc chúng đã được sửa đổi theo phương thức có kiểm soát với các quyền hợp thức.

Đặt các lỗi an toàn dưới CM đảm bảo rằng báo cáo về lỗi an toàn không bị mất hoặc bỏ quên, cho phép nhà phát triển theo dấu lỗi an toàn và giải quyết chúng.

13.2.7.2 Chú thích ứng dụng

ALC_CMS.4.1C đưa ra yêu cầu các lỗi an toàn được đưa vào danh sách cấu hình, và do vậy là chủ thể cho các yêu cầu CM về năng lực CM (ALC_CMC). Điều này đòi hỏi thông tin liên quan đến các lỗi an toàn trước đó và việc giải quyết chúng cần được duy trì, cũng như các chi tiết liên quan đến các lỗi an toàn hiện tại.

13.2.7.3 Phần tử hành động của nhà phát triển

13.2.7.3.1 ALC_CMS.4.1D

Nhà phát triển cần cung cấp một danh sách cấu hình cho TOE.

13.2.7.4 Các phần tử nội dung và trình bày

13.2.7.4.1 ALC_CMS.4.1C

Danh sách cấu hình cần chứa thông tin sau: bản thân TOE; bằng chứng đánh giá đòi hỏi bởi các SAR, tất cả các thành phần cấu thành TOE, biểu diễn triển khai TOE; **các báo cáo lỗi an toàn và trạng thái giải quyết**.

13.2.7.4.2 ALC_CMS.4.2C

Danh sách cấu hình cần xác định duy nhất các mục cấu hình.

13.2.7.4.3 ALC_CMS.4.3C

Đối với mỗi mục cấu hình liên quan TSF, danh sách cấu hình cần chỉ ra nhà phát triển của mục đó.

13.2.7.5 Các phần tử hành động của đánh giá viên

13.2.7.5.1 ALC_CMS.4.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.2.8 ALC_CMS.5 Các công cụ phát triển CM Tổng quát

Các mối phụ thuộc: Không có các mối phụ thuộc.

13.2.8.1 Mục tiêu

Một hệ thống CM có thể kiểm soát các thay đổi chỉ với các mục đã đưa vào CM (nghĩa là các mục cấu hình đã xác định trong danh sách cấu hình). Việc đặt bản thân TOE, các thành phần cấu thành TOE, và bằng chứng đánh giá yêu cầu bởi các SAR dưới CM đưa ra sự bảo đảm về việc chúng đã được sửa đổi theo phương thức có kiểm soát với các quyền hợp thức.

Đặt các lỗi an toàn dưới CM đảm bảo rằng báo cáo về lỗi an toàn không bị mất hoặc bỏ quên, cho phép nhà phát triển theo dấu lỗi an toàn và giải quyết chúng.

Các công cụ phát triển đóng một vai trò quan trọng nhằm đảm bảo sản xuất ra một phiên bản TOE chất lượng. Do đó, việc kiểm soát các sửa đổi các công cụ này là rất quan trọng.

13.2.8.2 Chú thích ứng dụng

ALC_CMS.5.1C đưa ra yêu cầu về việc các công cụ phát triển và thông tin liên quan được đưa vào danh sách cấu hình, và do vậy là chủ thể cho các yêu cầu CM về năng lực CM (ALC_CMC).

Ví dụ về các công cụ phát triển là các ngôn ngữ lập trình, các trình biên dịch. Thông tin gắn liền với các mục tạo ra TOE (như tùy chọn trình biên dịch, tùy chọn tạo phần mềm, tùy chọn tạo tệp thực thi) là ví dụ về thông tin liên quan đến các công cụ phát triển.

13.2.8.3 Phần tử hành động của nhà phát triển

13.2.8.3.1 ALC_CMS.5.1D

Nhà phát triển cần cung cấp một danh sách cấu hình cho TOE.

13.2.8.4 Các phần tử nội dung và trình bày

13.2.8.4.1 ALC_CMS.5.1C

Danh sách cấu hình cần chứa thông tin sau: bản thân TOE; bằng chứng đánh giá đòi hỏi bởi các SAR, tất cả các thành phần cấu thành TOE, biểu diễn triển khai TOE; các báo cáo lỗi an toàn và trạng thái giải quyết; **các công cụ phát triển và thông tin liên quan**.

13.2.8.4.2 ALC_CMS.5.2C

Danh sách cấu hình cần xác định duy nhất các mục cấu hình.

13.2.8.4.3 ALC_CMS.5.3C

Đối với mỗi mục cấu hình liên quan TSF, danh sách cấu hình cần chỉ ra nhà phát triển của mục đó.

13.2.8.5 Các phần tử hành động của đánh giá viên

13.2.8.5.1 ALC_CMS.5.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.3 Chuyển giao (ALC_DEL)

13.3.1 Mục tiêu

Mối quan tâm của họ này là truyền một cách an toàn TOE đã hoàn thiện từ môi trường phát triển sang trách nhiệm của người dùng.

Các yêu cầu cho chuyển giao đòi hỏi các phương tiện kiểm soát hệ thống và phân phối, các thủ tục chỉ ra chi tiết các biện pháp cần thiết nhằm đưa ra sự bảo đảm rằng an toàn của TOE được duy trì trong suốt quá trình phân phối TOE tới người dùng. Cho việc phân phối hợp lệ TOE, các thru tục sử dụng

cho phân phối TOE xem xét Mục tiêu đã xác định trong PP/ST liên quan đến an toàn của TOE trong chuyển giao.

13.3.2 Phân mức thành phần

Họ này chỉ chứa một thành phần. Mức tăng dần tính bảo vệ được tạo ra qua việc đòi hỏi tính tương xứng của các thủ tục chuyển giao với tiềm năng tấn công giả thiết có trong họ Phân tích điểm yếu (AVA_VAN).

13.3.3 Chú thích ứng dụng

Việc vận chuyển từ nhà thầu phụ tới nhà phát triển hoặc giữua các địa điểm phát triển khác nhau không được xem xét ở đây mà ở họ An toàn phát triển (ALC_DVS).

Kết thúc chu trình chuyển giao đánh dấu bởi việc vận chuyển TOE tới tay người dùng. Điều này không nhất nhiết phải có nghĩa là việc TOE đến tận địa điểm người dùng.

Các thủ tục chuyển giao cần xem xét, nếu có thể, các vấn đề sau:

a) đảm bảo rằng TOE được nhận bởi khách hàng tương ứng chính xác với phiên bản đã đánh giá của TOE;

b) tránh hoặc phát hiện các giả mạo với phiên bản thực tế của TOE;

c) ngăn chặn gửi phiên bản TOE sai;

d) tránh phân phối TOE một cách quá lộ liễu tới khách hàng: có thể xem những trường hợp hạn chế tin tặc biết rõ về việc TOE được chuyển giao khi nào và như thế nào;

e) tránh hoặc phát hiện việc TOE bị can thiệp trong quá trình chuyển giao;

f) tránh việc gửi TOE bị trễ hoặc chặn khi phân phối.

Các thủ tục chuyển giao cần đưa ra các hành động của người nhận sẵn sàng đối với các vấn đề trên. Mô tả nhất quán các hành động sẵn sàng nêu trên được kiểm tra trong họ "Các thủ tục chuẩn bị" (AGD_PRE), nếu có.

13.3.4 ALC_DEL.1 Các thủ tục chuyển giao

Các mối phụ thuộc: Không có các mối phụ thuộc.

13.3.4.1 Phần tử hành động của nhà phát triển

13.3.4.1.1 ALC_DEL.1.1D

Nhà phát triển cần văn bản hóa các thủ tục chuyển giao TOE hoặc các thành phần của nó tới người tiêu dùng.

13.3.4.1.2 ALC_DEL.2.1D

Nhà phát triển cần sử dụng các thủ tục chuyển giao.

13.3.4.2 Các phần tử nội dung và trình bày

13.3.4.2.1 ALC_DEL.1.1C

Tài liệu chuyển giao cần mô tả mọi thủ tục cần thiết để duy trì an toàn khi phân phối các phiên bản TOE tới người tiêu dùng.

13.3.4.3 Các phần tử hành động của đánh giá viên

13.3.4.3.1 ALC_DEL.1.1E

Đánh giá viên cần xác nhận rằng thông tin đưa ra thỏa mãn tất cả các yêu cầu về nội dung và sự thể hiện bằng chứng.

13.4 An toàn phát triển (ALC_DVS)

13.4.1 Mục tiêu

An toàn phát triển liên quan đến các biện pháp vật lý, quy trình, nhân sự và các biện pháp an toàn khác có thể dùng trong môi trường phát triển nhằm bảo vệ TOE và các thành phần của nó. Nó bao gồm an toàn vật lý cho địa điểm phát triển, các quy trình dùng để chọn lựa nhân viên phát triển.

13.4.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở có cần điều chỉnh về việc các biện pháp an toàn đã đầy đủ hay chưa.

13.4.3 Chú thích ứng dụng

Họ này liên quan đến các biện pháp nhằm loại bỏ hoặc giảm thiểu nguy cơ tồn tại ở phía nhà phát triển.

Đánh giá viên nên tham quan các địa điểm nhằm đánh giá chứng cứu về an toàn phát triển. Việc này có thể bao gồm các địa điểm của các nhà thầu phụ liên quan đến phát triển và sản xuất TOE. Mọi quyết định về việc không đến tham quan cần được phép của cơ quan đánh giá.

Mặc dù an toàn phát triển liên quan đến việc duy trì TOE và do vậy đến các yếu tố có thể liên quan sau khi kết thúc đánh giá, các yêu cầu An toàn phát triển (ALC_DVS) chỉ đặc trưng rằng các biện pháp an toàn phát triển đã có ở thời điểm đánh giá. Ngoài ra an toàn phát tiển (ALC_DVS) không chứa bất kỳ yêu cầu nào liên quan đến ý định của nhà tài trợ về việc áp dụng các biện pháp an toàn phát triển trong tương lai, sau khi kết thúc đánh giá.

Có thể thấy là tính tin cậy không phải lúc nào cũng là vấn đề đối với việc bảo vệ TOE trong môi trường phát triển. Việc sử dụng từ "cần thiết" cho phép chọn lựa sự bảo vệ phù hợp.

13.4.4 ALC_DVS.1 Định danh các biện pháp an toàn

Các mối phụ thuộc: không có sự phụ thuộc nào

13.4.4.1 Phần tử hành động của nhà phát triển

13.4.4.1.1 ALC_DVS.1.1D

Nhà phát triển cần tạo ra tài liệu an toàn phát triển.

13.4.4.2 Các phần tử nội dung và trình bày

13.4.4.2.1 ALC_DVS.1.1C

Tài liệu an toàn phát triển cần mô tả tất cả các biện pháp vật lý, thủ tục, nhân sự và các biện pháp an toàn khác cần thiết để bảo vệ tính tin cậy và tính toàn vẹn của thiết kế và thực thi TOE trong môi trường phát triển của nó.

13.4.4.3 Các phần tử hành động của đánh giá viên

13.4.4.3.1 ALC_DVS.1.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.4.4.3.2 ALC_DVS.1.2E

Đánh giá viên cần khẳng định rằng các biện pháp an toàn đang được áp dụng.

13.4.5 ALC_DVS.2 Sự đầy đủ các biện pháp an toàn

Các mối phụ thuộc: không có sự phụ thuộc nào.

13.4.5.1 Phần tử hành động của nhà phát triển

13.4.5.1.1 ALC_DVS.2.1D

Nhà phát triển cần tạo ra tài liệu an toàn phát triển

13.4.5.2 Các phần tử nội dung và trình bày

13.4.5.2.1 ALC_DVS.2.1C

Tài liệu an toàn phát triển cần mô tả tất cả các biện pháp vật lý, thủ tục, nhân sự và các biện pháp an toàn khác mà cần để bảo vệ tính tin cậy và tính toàn vẹn của thiết kế và thực thi TOE trong môi trường phát triển của nó.

13.4.5.2.2 ALC_DVS.2.2C

Tài liệu an toàn phát triển cần biện minh về việc các biện pháp an toàn đưa ra mức độ bảo vệ cần thiết nhằm duy trì tính tin cậy và toàn vẹn cho TOE.

13.4.5.3 Các phần tử hành động của đánh giá viên

13.4.5.3.1 ALC_DVS.2.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.4.5.3.2 ALC_DVS.2.2E

Đánh giá viên cần khẳng định rằng các biện pháp an toàn đang được áp dụng.

13.5 Sửa lỗi (ALC_FLR)

13.5.1 Mục tiêu

Sửa lỗi yêu cầu các lỗi an toàn phát hiện được phải do nhà phát triển lần theo dấu vết và sửa chữa. Dù cho sự tương thích tương lai với các thủ tục sửa lỗi không thể xác định được tại thời điểm đánh giá TOE, thì vẫn có thể đánh giá các thủ tục và chính sách mà nhà phát triển đang có để lần theo dấu vết và sửa lỗi, và để phân loại các chỉnh sửa và thông tin lỗi.

13.5.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở của việc mở rộng phạm vi các thủ tục sửa lỗi và tính chính xác của các thủ tục sửa lỗi.

13.5.3 Chú thích ứng dụng

Họ này đảm bảo rằng TOE được bảo hành và hỗ trợ trong tương lai, yêu cầu nhà phát triển TOE lần theo dấu vết và sửa các lỗi trong TOE. Hơn nữa, các yêu cầu được kèm theo khi phân loại sửa lỗi. Tuy nhiên, họ này không áp đặt các yêu cầu đánh giá ngoài đánh giá hiện tại.

Người sử dụng TOE được coi là tâm điểm của đơn vị sử dụng mà chịu trách nhiệm nhận và thực hiện chữa các lỗi an toàn. Đó không cần phải là cá nhân người sử dụng, mà có thể là đại diện của tổ chức

người chịu trách nhiệm khắc phục lỗi an toàn. Việc sử dụng thuật ngữ người sử dụng TOE nhận ra rằng các tổ chức khác nhau có các thủ tục khác nhau trong xử lý báo cáo lỗi, mà có thể do cá nhân người sử dụng hoặc do một cơ quan quản lý trung tâm thực hiện.

Các thủ tục sửa lỗi cần mô tả các phương pháp để xử lý với tất cả các kiểu lỗi gặp phải. Các lỗi này có thể do nhà phát triển, do những người sử dụng của TOE, hoặc các bên khác quen thuộc với TOE báo cáo. Một số lỗi có thể không được sửa ngay lập tức. Có thể có một số trường hợp mà lỗi không thể xử lý được ngay mà phải thực hiện các biện pháp khác (ví dụ biện pháp thủ tục). Những tài liệu ghi lại được đưa ra có thể khôi phục các thủ tục để cung cấp cho nơi vận hành các xử lý, và cung cấp thông tin về các lỗi mà việc xử lý đã hoãn lại (và làm gì trong tạm thời) hoặc khi mà việc sửa chữa là không thể.

Các thay đổi đối với TOE sau khi phát hành được coi là chưa đánh giá; mặc dù một số thông tin từ bản đánh giá chính thức vẫn có thể áp dụng. Cụm từ "phát hành TOE" dùng trong họ này do đó tham chiếu đến một phiên bản của một sản phẩm là phát hành một TOE đã chứng nhận với các thay đổi đã áp dụng.

13.5.4 ALC_FLR.1 Sửa lỗi cơ bản

Tính Các mối phụ thuộc: không có sự phụ thuộc nào

13.5.4.1 Phần tử hành động của nhà phát triển

13.5.4.1.1 ALC_FLR.1.1D

Nhà phát triển cần văn bản hóa các thủ tục sửa lỗi chỉ định cho nhà phát triển TOE.

13.5.4.2 Các phần tử nội dung và trình bày

13.5.4.2.1 ALC_FLR.1.1C

Tài liệu các thủ tục sửa lỗi cần mô tả các thủ tục được sử dụng để theo dấu tất cả các lỗi an toàn đã báo cáo trong mỗi phát hành của TOE.

13.5.4.2.2 ALC_FLR.1.2C

Các thủ tục sửa lỗi cần yêu cầu việc mô tả bản chất và ảnh hưởng của từng lỗi an toàn được cung cấp, cũng như hiện trạng tìm thấy cách sửa lỗi đó.

13.5.4.2.3 ALC_FLR.1.3C

Các thủ tục sửa lỗi cần yêu cầu các hành động sửa chữa được xác định cho từng lỗi an toàn.

13.5.4.2.4 ALC_FLR.1.4C

Tài liệu các thủ tục sửa lỗi cần mô tả các phương pháp sử dụng để cung cấp thông tin, sửa chữa, hướng dẫn về các hành động sửa lỗi cho người sử dụng TOE.

13.5.4.3 Các phần tử hành động của đánh giá viên

13.5.4.3.1 ALC_FLR.1.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.5.5 ALC_FLR.2 Các thủ tục báo cáo lỗi

Tính Các mối phụ thuộc: không có sự phụ thuộc nào.

13.5.5.1 Mục tiêu

Để nhà phát triển có thể hành động phù hợp với các báo cáo lỗi an toàn từ những người sử dụng TOE, và để biết ai gửi các xử lý sửa chữa, người sử dụng TOE cần hiểu cách gửi báo cáo lỗi an toàn tới nhà phát triển thế nào. Hướng dẫn sửa lỗi từ nhà phát triển tới người sử dụng TOE đảm bảo rằng những người sử dụng TOE nhận thức được thông tin quan trọng này.

13.5.5.2 Phần tử hành động của nhà phát triển

13.5.5.2.1 ALC_FLR.2.1D

Nhà phát triển cần văn bản hóa các thủ tục sửa lỗi chỉ định cho nhà phát triển TOE.

13.5.5.2.2 ALC_FLR.2.2D

Nhà phát triển cần tạo ra một thủ tục để chấp nhận và hành động khi có mọi báo cáo lỗi an toàn và các yêu cầu sửa chữa đối với các lỗi đó.

13.5.5.2.3 ALC_FLR.2.3D

Nhà phát triển cần cung cấp hướng dẫn sửa lỗi chỉ định cho người sử dụng TOE

13.5.5.3 Các phần tử nội dung và trình bày

13.5.5.3.1 ALC_FLR.2.1C

Tài liệu các thủ tục sửa lỗi cần mô tả các thủ tục được sử dụng để lần theo dấu vết tất cả các lỗi an toàn đã báo cáo trong mỗi phát hành của TOE.

13.5.5.3.2 ALC_FLR.2.2C

Các thủ tục sửa lỗi cần yêu cầu việc mô tả bản chất và ảnh hưởng của từng lỗi an toàn được cung cấp, cũng như hiện trạng tìm thấy cách sửa lỗi đó.

13.5.5.3.3 ALC_FLR.2.3C

Các thủ tục sửa lỗi cần yêu cầu các hành động sửa chữa được xác định cho từng lỗi an toàn.

13.5.5.3.4 ALC_FLR.2.4C

Tài liệu các thủ tục sửa lỗi cần mô tả các phương pháp được sử dụng để cung cấp hướng dẫn, sửa chữa, thông tin lỗi trong các hành động sửa lỗi cho người sử dụng TOE.

13.5.5.3.5 ALC_FLR.2.5C

Các thủ tục sửa lỗi cần mô tả các phương thức nhà phát triển nhận các báo cáo từ người sử dụng TOE và các yêu cầu về lỗi an toàn nghi ngờ trong TOE.

13.5.5.3.6 ALC_FLR.2.6C

Các thủ tục xử lý các lỗi an toàn đã báo cáo cần đảm bảo rằng bất cứ lỗi đã báo cáo nào đang được sửa và việc sửa chữa đã được báo cho người dùng TOE.

13.5.5.3.7 ALC_FLR.2.7C

Các thủ tục xử lý lỗi an toàn đã báo cáo cần cung cấp sự bảo vệ an toàn sao cho bất cứ sửa chữa nào đối với lỗi an toàn này không làm nảy sinh các lỗi nào mới.

13.5.5.3.8 ALC_FLR.2.8C

Hướng dẫn sửa lỗi cần mô tả các phương thức người sử dụng TOE báo cáo cho nhà phát triển về bất cứ lỗi an toàn khả nghi nào trong TOE.

13.5.5.4 Các phần tử hành động của đánh giá viên

13.5.5.4.1 ALC_FLR.2.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.5.6 ALC_FLR.3 Sửa lỗi hệ thống

Các mối phụ thuộc: không có sự phụ thuộc nào.

13.5.6.1 Mục tiêu

Để nhà phát triển có thể hành động phù hợp với các báo cáo lỗi an toàn từ những người sử dụng TOE, và để biết ai gửi các xử lý sửa chữa, người sử dụng TOE cần hiểu cách gửi báo cáo lỗi an toàn tới nhà phát triển thế nào. Hướng dẫn sửa lỗi từ nhà phát triển tới người sử dụng TOE đảm bảo rằng những người sử dụng TOE nhận thức được thông tin quan trọng này.

13.5.6.2 Phần tử hành động của nhà phát triển

13.5.6.2.1 ALC_FLR.3.1D

Nhà phát triển cần văn bản hóa các thủ tục sửa lỗi chỉ định cho nhà phát triển TOE.

13.5.6.2.2 ALC_FLR.3.2D

Nhà phát triển cần tạo ra một thủ tục để chấp nhận và hành động khi có mọi báo cáo lỗi an toàn và các yêu cầu sửa chữa đối với các lỗi đó.

13.5.6.2.3 ALC_FLR.3.3D

Nhà phát triển cần cung cấp hướng dẫn sửa lỗi chỉ định cho người sử dụng TOE

13.5.6.3 Các phần tử nội dung và trình bày

13.5.6.3.1 ALC_FLR.3.1C

Tài liệu các thủ tục sửa lỗi cần mô tả các thủ tục được sử dụng để lần theo dấu vết tất cả các lỗi an toàn đã báo cáo trong mỗi phát hành của TOE.

13.5.6.3.2 ALC_FLR.3.2C

Các thủ tục sửa lỗi cần yêu cầu việc mô tả bản chất và ảnh hưởng của từng lỗi an toàn được cung cấp, cũng như hiện trạng tìm thấy cách sửa lỗi đó.

13.5.6.3.3 ALC_FLR.3.3C

Các thủ tục sửa lỗi cần yêu cầu các hành động sửa chữa được xác định cho từng lỗi an toàn.

13.5.6.3.4 ALC_FLR.3.4C

Tài liệu các thủ tục sửa lỗi cần mô tả các phương pháp được sử dụng để cung cấp hướng dẫn, sửa chữa, thông tin lỗi trong các hành động sửa lỗi cho người sử dụng TOE.

13.5.6.3.5 ALC_FLR.3.5C

Các thủ tục sửa lỗi cần mô tả các phương thức nhà phát triển nhận các báo cáo từ người sử dụng TOE và các yêu cầu về lỗi an toàn nghi ngờ trong TOE.

13.5.6.3.6 ALC_FLR.3.6C

Các thủ tục xử lý các lỗi an toàn đã báo cáo cần gồm một thủ tục yêu cầu phản hồi kịp thời và phân phối tự động các báo cáo lỗi an toàn cũng như các sửa đổi liên quan tới người dùng đã đăng ký đã có thể chịu ảnh hưởng của lỗi an toàn.

13.5.6.3.7 ALC_FLR.3.7C

Các thủ tục xử lý các lỗi an toàn đã báo cáo cần đảm bảo rằng bất cứ lỗi đã báo cáo nào đang được sửa và việc sửa chữa đã được báo cho người dùng TOE.

13.5.6.3.8 ALC_FLR.3.8C

Các thủ tục xử lý lỗi an toàn đã báo cáo cần cung cấp sự bảo vệ an toàn sao cho bất cứ sửa chữa nào đối với lỗi an toàn này không làm nảy sinh các lỗi nào mới.

13.5.6.3.9 ALC_FLR.3.9C

Hướng dẫn sửa lỗi cần mô tả các phương thức người sử dụng TOE báo cáo cho nhà phát triển về bất cứ lỗi an toàn khả nghi nào trong TOE.

13.5.6.3.10 ALC_FLR.3.10C

Hướng dẫn sửa lỗi cần mô tả phương thức người dùng TOE có thể đăng ký với nhà phát triển nhằm có thể nhận được các báo cáo và sửa chữa lỗi an toàn một cách hợp thức.

13.5.6.3.11 ALC_FLR.3.11C

Hướng dẫn sửa lỗi cần xác định các đầu mối liên lạc cụ thể cho tất cả các báo cáo và yêu cầu về các vấn đề an toàn liên quan đến TOE.

13.5.6.4 Các phần tử hành động của đánh giá viên

13.5.6.4.1 ALC_FLR.3.1E

Đánh giá viên sẽ khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.6 Định nghĩa vòng đời (ALC_LCD)

13.6.1 Mục tiêu

Việc phát triển và duy trì TOE với kiểm soát nghèo nàn có thể mang lại một TOE không đáp ứng được tất cả các yêu cầu an toàn SFRs của nó. Do đó, điều quan trọng là cần tạo ra một mô hình cho phát triển và duy trì TOE càng sớm càng tốt trong vòng đời của TOE.

Sử dụng một mô hình cho việc phát triển và duy trì TOE không bảo đảm rằng TOE đáp ứng được tất cả các yêu cầu chức năng an toàn SFRs của nó. Có thể là một mô hình được chọn sẽ thiếu hoặc không thoả đáng và do đó sẽ không thấy lợi ích về chất lượng của TOE. Việc sử dụng một mô hình vòng đời đã được một số nhóm các chuyên gia phê duyệt (vi dụ các chuyên gia hàn lâm, các cơ quan định chuẩn) làm tăng cơ hội cho các mô hình phát triển và duy trì nhằm làm cho TOE đáp ứng các SFRs của nó. Sử dụng một mô hình vòng đời bao hàm một số định lượng sẽ làm tăng tính đảm bảo về chất lượng chung của quy trình phát triển TOE.

13.6.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở các yêu cầu tăng dần về định lượng của mô hình vòng đời, và việc tương thích với mô hình đó.

13.6.3 Chú thích ứng dụng

Một mô hình vòng đời chứa đựng các thủ tục, công cụ và kỹ thuật được sử dụng để phát triển và duy trì TOE. Các khía cạnh của quá trình có thể được bao hàm bởi một mô hình như vậy gồm các phương pháp thiết kế, các thủ tục soát xét, các biện pháp quản lý dự án, các thủ tục kiểm soát thay đổi, các phương pháp kiểm thử và các thủ tục chấp nhận. Một mô hình vòng đời hiệu quả sẽ chỉ ra những khía cạnh này của quá trình phát triển và duy trì này trong một cấu trúc quản lý tổng thể chỉ định trách nhiệm và qui trình giám sát.

Có nhiều kiểu tình huống chấp thuận khác nhau liên quan đến các vị trí khác nhau trong tiêu chí: chấp thuận các thành phần chuyển giao từ các nhà thầu phụ ("tích hợp") nên được xem trong họ Định nghĩa vòng đời (ALC_LCD) này, chấp thuận liên quan đến vận chuyển nội bộ trong An toàn phát triển (ALC_DVS), chấp thuận các thành phần vào hệ thống CM trong năng lực CM (ALC_CMC), chấp thuận của người tiêu dùng với TOE đã chuyển giao trong họ Chuyển giao (ALC_DEL). Ba kiểu đầu tiên có thể giao nhau.

Mặc dù định nghĩa vòng đời liên quan đến duy trì TOE và do đó các khía cạnh trở lên thích hợp sau khi hoàn tất việc đánh giá, việc đánh giá nó bổ sung thêm sự đảm bảo thông qua phân tích thông tin vòng đời cho TOE được cung cấp tại thời điểm đánh giá.

Một mô hình vòng đời cung cấp biện pháp quản lý cần thiết trogn phát triển và duy trì TOE, nếu mô hình cho phép tối thiểu hóa vừa đủ nguy cơ TOE không đáp ứng yêu cầu an toàn của nó.

Một mô hình vòng đời là mô hình dùng một số giá trị định lượng (tham số số học và/ hoặc số đo) cho sản phẩm được quản lý nhằm đo lường các đặc điểm phát triển sản phẩm. Các số đo điển hình là số đo độ phức tạp của mã nguồn, mật độ lỗi (số lỗi trên kích thước mã nguồn) hoặc thời gian lỗi trung bình. Đối với đánh giá an toàn, mọi số đo trên đều phù hợp, chúng được sử dụng để tăng chất lượng bằng cách giảm xác suất lỗi, do đó tăng tính bảo đảm an toàn cho TOE.

Cần lưu ý một điều là sẵn có các mô hình vòng đời tiêu chuẩn (ví dụ mô hình thác nước), mặt khác cũng có các đại lượng đo tiêu chuẩn (ví dụ mật độ lỗi) và chúng có thể kết hợp với nhau. TCVN 8709 không yêu cầu vòng đời phải tuân theo chính xác một tiêu chuẩn phản ánh cả hai khía cạnh trên.

13.6.4 ALC-LCD.1 Mô hình vòng đời định nghĩa bởi nhà phát triển

Các mối phụ thuộc: không có sự phụ thuộc nào

13.6.4.1 Phần tử hành động của nhà phát triển

13.6.4.1.1 ALC_LCD.1.1D

Nhà phát triển cần tạo ra mô hình vòng đời được sử dụng trong phát triển và duy trì của TOE

13.6.4.1.2 ALC_LCD.1.2D

Nhà phát triển cần cung cấp tài liệu định nghĩa vòng đời.

13.6.4.2 Các phần tử nội dung và trình bày

13.6.4.2.1 ALC_LCD.1.1C

Tài liệu định nghĩa vòng đời cần mô tả mô hình được sử dụng để phát triển và duy trì TOE.

13.6.4.2.2 ALC_LCD.1.2C

Mô hình vòng đời cần cung cấp kiểm soát cần thiết cho việc phát triển và duy trì TOE.

13.6.4.3 Các phần tử hành động của đánh giá viên

13.6.4.3.1 ALC_LCD.1.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.6.5 ALC_LCD.2 Mô hình vòng đời định lượng

Tính Các mối phụ thuộc: không có sự phụ thuộc nào

13.6.5.1 Phần tử hành động của nhà phát triển

13.6.5.1.1 ALC_LCD.2.1D

Nhà phát triển cần tạo ra mô hình vòng đời được sử dụng trong phát triển và duy trì của TOE, **và nó được dựa trên một mô hình vòng đời định lượng.**

13.6.5.1.2 ALC_LCD.2.2D

Nhà phát triển cần cung cấp tài liệu định nghĩa vòng đời.

13.6.5.1.3 ALC_LCD.2.3D

Nhà phát triển cần đo lường việc phát triển TOE sử dụng một mô hình vòng đời định lượng.

13.6.5.2 Nội dung và trình bày của phần tử chứng cớ

13.6.5.2.1 ALC_LCD.2.1C

Tài liệu định nghĩa vòng đời cần mô tả mô hình được sử dụng để phát triển và duy trì TOE, **bao gồm các chi tiết về tham số sô học của nó và/hoặc các số đo dùng để đo lường chất lượng TOE và/hoặc việc phát triển nó.**

13.6.5.2.2 ALC_LCD.2.2C

Mô hình vòng đời cần cung cấp kiểm soát cần thiết cho việc phát triển và duy trì TOE.

13.6.5.2.3 ALC_LCD 2.3C

Tài liệu đầu ra của vòng đời cần đưa ra kết quả về các phép đo sự phát triển TOE với mô hình vòng đời định lượng.

13.6.5.3 Phần tử hành động đánh giá viên

13.6.5.3.1 ALC_LCD.2.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.7 Các công cụ và các kỹ thuật (ALC_TAT)

13.7.1 Mục tiêu

Các công cụ và kỹ thuật là một khía cạnh chọn lựa công cụ được sử dụng để phát triển, phân tích và triển khai TOE. Nó bao gồm các yêu cầu tránh các công cụ phát triển không đúng, mâu thuẫn, mập mờ

khi sử dụng phát triển TOE. Điều này bao gồm, nhưng không giới hạn, cả các ngôn ngữ lập trình, tài liệu, các chuẩn triển khai, các thành phần khác của TOE vi như là hỗ trợ thư viện thời gian thực.

13.7.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở các yêu cầu tăng dẫn về mô tả và phạm vi của các tiêu chuẩn triển khai và tài liệu về các tùy chọn phụ thuộc triển khai.

13.7.3 Chú thích ứng dụng

Có một yêu cầu đối với các công cụ phát triển được xác định rõ. Đó là các công cụ được mô tả rõ ràng và đầy đủ. Ví dụ, các ngôn ngữ lập trình và các hệ thông thiết kế có trợ giúp của máy tính (CAD) chúng đều dựa trên một tiêu chuẩn đã công bố bởi các cơ quan tiêu chuẩn và được xem là xác định rõ. Các công cụ tự làm cần được xem xét thêm nhằm làm rõ chúng có thuộc loại xác định rõ hay không.

Yêu cầu trong ALC_TAT.1.2C được áp dụng đặc biệt cho các ngôn ngữ lập trình để đảm bảo rằng tất cả các tuyên bố trong mã nguồn đều có một nghĩa rõ ràng.

Trong ALC_TAT.2 và ALC_TAT.3, các hướng dẫn triển khai có thể được chấp nhận làm tiêu chuẩn triển khai nếu như chúng được phê chuẩn bởi một số nhóm chuyên gia (ví dụ chuyên gia khoa học, các cơ quan tiêu chuẩn). Các tiêu chuẩn triển khai thường công khai, được chấp thuận rộng rãi và thực hành chung trong một lĩnh vực đặc trưng, tuy nhiên các hướng dẫn triển khai đặc trưng của nhà phát triển cũng có thể được chấp nhận làm tiêu chuẩn; quan trọng là ý kiến chuyên gia.

Các công cụ và kỹ thuật phân biệt giữa các tiêu chuẩn triển khai áp dụng bởi nhà phát triển (ALC_TAT.2.3D) và các tiêu chuẩn triển khai cho "mọi thành phần TOE" (ALC_TAT.3.3D) trong đó bao gồm phần mềm, phần cứng hoặc phần sụn của bên thứ ba. Danh sách cấu hình có trong phạm vi CM (ALC_CMS) đòi hỏi rằng mỗi mục cấu hình tương ứng TSF biểu thị việc nó được tạo ra bởi nhà phát triển TOE hay nhà phát triển bên thứ ba.

13.7.4 ALC_TAT.1 Các công cụ phát triển được định nghĩa rõ ràng

Các mối phụ thuộc: ADV_IMP.1 Biểu diễn triển khai của TSF

13.7.4.1 Phần tử hành động của nhà phát triển

13.7.4.1.1 ALC_TAT.1.1D

Nhà phát triển cần xác định mọi công cụ phát triển được sử dụng cho TOE

13.7.4.1.2 ALC_TAT.1.2D

Nhà phát triển cần văn bản hóa các tùy chọn phụ thuộc triển khai đã được lựa chọn cho mỗi công cụ phát triển.

13.7.4.2 Các phần tử nội dung và trình bày

13.7.4.2.1 ALC_TAT.1.1C

Mọi công cụ phát triển sử dụng cho triển khai cần xác định rõ ràng.

13.7.4.2.2 ALC_TAT.1.2C

Tài liệu cho mỗi công cụ phát triển cần định nghĩa rõ ràng ý nghĩa của tất cả các tuyên bố cũng như các quy ước và các chỉ dẫn sử dụng trong triển khai.

13.7.4.2.3 ALC_TAT.1.3C

Tài liệu cho mỗi công cụ phát triển cần định nghĩa rõ ràng ý nghĩa của tất cả các tùy chọn phụ thuộc triển khai.

13.7.4.3 Các phần tử hành động của đánh giá viên

13.7.4.3.1 ALC_TAT.1.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.7.5 ALC_TAT.2 Tương thích với các tiêu chuẩn triển khai

Các mối phụ thuộc: ADV_IMP.1 Biểu diễn triển khai của TSF

13.7.5.1 Phần tử hành động của nhà phát triển

13.7.5.1.1 ALC_TAT.2.1D

Nhà phát triển cần xác định mọi công cụ phát triển sử dụng cho TOE

13.7.5.1.2 ALC_TAT.2.2D

Nhà phát triển cần văn bản hóa các tùy chọn phụ thuộc triển khai đã được lựa chọn cho mỗi công cụ phát triển.

13.7.5.1.3 ALC_TAT.2.3D

Nhà phát triển cần mô tả các tiêu chuẩn triển khai đang được nhà phát triển áp dụng.

13.7.5.2 Các phần tử nội dung và trình bày

13.7.5.2.1 ALC_TAT.2.1C

Mọi công cụ phát triển sử dụng cho triển khai cần xác định rõ ràng.

13.7.5.2.2 ALC_TAT.2.2C

Tài liệu cho mỗi công cụ phát triển cần định nghĩa rõ ràng ý nghĩa của tất cả các tuyên bố cũng như các quy ước và các chỉ dẫn sử dụng trong triển khai.

13.7.5.2.3 ALC_TAT 2.3C

Tài liệu cho mỗi công cụ phát triển cần định nghĩa rõ ràng ý nghĩa của tất cả các tùy chọn phụ thuộc triển khai.

13.7.5.3 Các phần tử hành động của đánh giá viên

13.7.5.3.1 ALC_TAT.2.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.7.5.3.2 ALC_TAT.2.2E

Đánh giá viên cần khẳng định rằng các tiêu chuẩn triển khai đã được áp dụng.

13.7.6 ALC_TAT.3 Tương thích với tiêu chuẩn triển khai - tất cả các thành phần.

Tính phụ thuộc: ADV_IMP.1 Biểu diễn triển khai của TSF

13.7.6.1 Phần tử hành động của nhà phát triển

13.7.6.1.1 ALC_TAT.3.1D

Nhà phát triển cần xác định mọi công cụ phát triển sử dụng cho TOE

13.7.6.1.2 ALC_TAT.3.2D

Nhà phát triển cần văn bản hóa các tùy chọn phụ thuộc triển khai đã được lựa chọn cho mỗi công cụ phát triển.

13.7.6.1.3 ALC_TAT.3.3D

Nhà phát triển cần mô tả các tiêu chuẩn triển khai đang được nhà phát triển áp dụng **và đang được áp dụng bởi mọi nhà cung cấp thứ ba cho mọi thành phần của TOE**.

13.7.6.2 Các phần tử nội dung và trình bày

13.7.6.2.1 ALC_TAT.3.1C

Mọi công cụ phát triển sử dụng cho triển khai cần xác định rõ ràng.

13.7.6.2.2 ALC_TAT 3.2C

Tài liệu cho mỗi công cụ phát triển cần định nghĩa rõ ràng ý nghĩa của tất cả các tuyên bố cũng như các quy ước và các chỉ dẫn sử dụng trong triển khai.

13.7.6.2.3 ALC_TAT 3.3C

Tài liệu cho mỗi công cụ phát triển cần định nghĩa rõ ràng ý nghĩa của tất cả các tùy chọn phụ thuộc triển khai.

13.7.6.3 Các phần tử hành động của đánh giá viên

13.7.6.3.1 ALC_TAT.3.1E

Đánh giá viên cần khẳng định rằng thông tin được cung cấp đáp ứng được tất cả các yêu cầu về nội dung và trình bày chứng cớ.

13.7.6.3.2 ALC_TAT.3.2E

Đánh giá viên cần khẳng định rằng các tiêu chuẩn triển khai đã được áp dụng.

14 Lớp ATE: Các kiểm thử

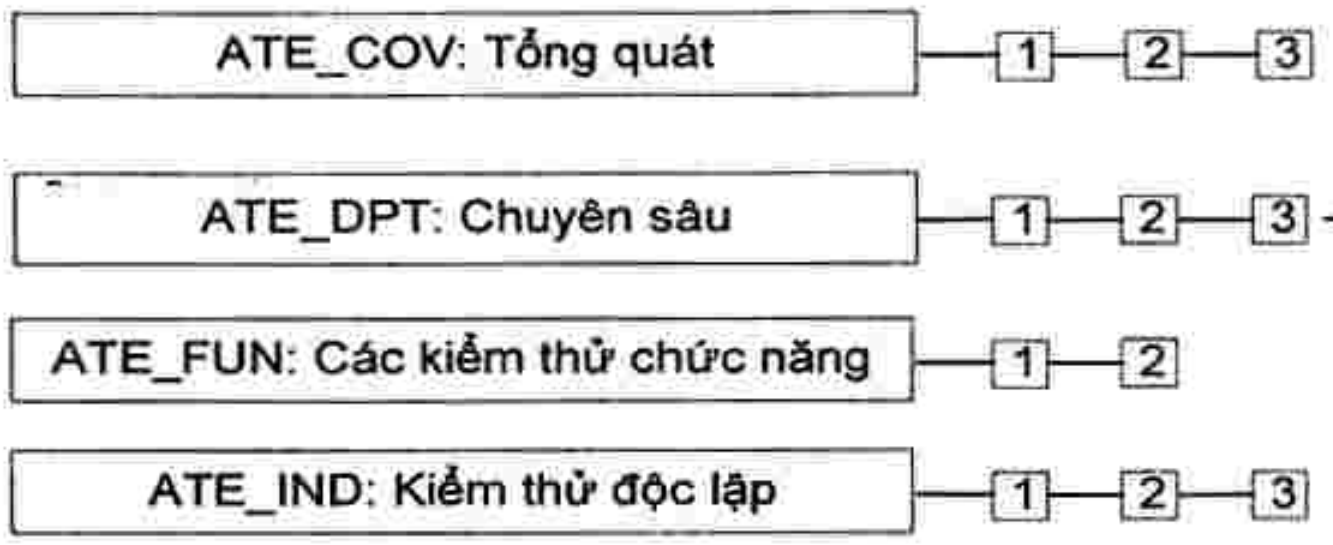
Lớp "Các kiểm thử" bao gồm 4 họ chính: Tổng quát (ATE_COV), Chuyên sâu (ATE_DPT), Kiểm thử độc lập (ATE_IND) (ví dụ kiểm thử chức năng bởi đánh giá viên) và Kiểm thử chức năng (ATE_FUN). Việc kiểm thử nhằm đảm bảo rằng TSF vận hành như đã mô tả (trong đặc tả chức năng, thiết kế TOE, và triển khai mẫu).

Điểm nhấn trong lớp này là khẳng định rằng TSF hoạt động theo như các mô tả thiết kế của nó. Lớp này không đề cập đến kiểm thử thâm nhập dựa trên việc phân tích TSF theo các tìm kiếm đặc trưng nhằm xác định các điểm yếu trong thiết kế và thực thi TSF. Kiểm thử thâm nhập được đề cập riêng trong mục đánh giá điểm yếu ở lớp AVA: đánh giá điểm yếu.

ATE: Lớp các kiểm thử phân chia việc kiểm thử thành các kiểm thử bởi nhà phát triển và các kiểm thử bởi đánh giá viên. Nhóm tổng quát (ATE_COV) và Chuyên sâu (ATE_DPT) đề cập đến tính đầy đủ của các kiểm thử bởi nhà phát triển. Tổng quát (ATE_COV) đề cập đến tính chặt chẽ cùng với đặc tả chức năng đã được kiểm thử; Chuyên sâu (ATE_DPT) đề cập đến việc có nên kiểm thử căn cứ vào các mô tả thiết kế khác (kiến trúc an toàn, thiết kế TOE, triển khai mẫu) đã được yêu cầu hay không.

Các kiểm thử chức năng đề cập đến việc thực hiện các kiểm thử bởi nhà phát triển và cách thức ghi lại bằng văn bản cho kiểm thử này như thế nào. Cuối cùng, kiểm thử độc lập (ATE_IND) đề cập đến việc kiểm thử bởi đánh giá viên: đánh giá viên nên lặp lại từng phần việc hoặc toàn bộ quá trình kiểm thử bởi nhà phát triển và bao nhiêu phép kiểm thử độc lập nên thực hiện.

Hình 14 trình bày các họ thuộc lớp này, và phân lớp các thành phần bên trong các họ.



Hình 14 - Phân rã lớp ATE: Kiểm thử

14.1 Tổng quát (ATE_COV)

14.1.1 Mục tiêu

Họ này xác minh rằng TSF đã được kiểm thử theo đặc tả chức năng của nó. Điều này đạt được thông qua việc kiểm tra chứng cứ tương ứng của nhà phát triển.

14.1.2 Phân mức thành phần

Các thành phần trong họ này được phân mức dựa vào đặc tả.

14.1.3 Chú thích ứng dụng

14.1.4 ATE_COV.1 Chứng cứ tổng quát

Các phụ thuộc: ADV_FSP.2 Đặc tả chức năng thực thi an toàn

ATE_FUN.1 Kiểm thử chức năng

14.1.4.1 Mục tiêu

Mục tiêu của thành phần này là việc một số các TSFI đã được kiểm thử.

14.1.4.2 Chú thích ứng dụng

Trong thành phần này nhà phát triển chỉ ra các kiểm thử trong tài liệu kiểm thử tương ứng với các TSFI trong đặc tả chức năng như thế nào. Điều này có thể đạt được với một khai báo tương hợp, có thể sử dụng một bảng.

14.1.4.3 Phần tử hành động của nhà phát triển

14.1.4.3.1 ATE_COV.1.1D

Nhà phát triển cần đưa ra được chứng cứ của tổng quan kiểm thử.

14.1.4.4 Các phần tử nội dung và trình bày

14.1.4.4.1 ATE_COV.1.1C

Chứng cứ của tổng quan kiểm thử cần chỉ ra sự tương ứng giữa các kiểm thử trong tài liệu kiểm thử và các TSFI trong đặc tả chức năng.

14.1.4.5 Các phần tử hành động của đánh giá viên

14.1.4.5.1 ATE_COV.1.1E

Đánh giá viên sẽ xác nhận rằng thông tin đưa ra đáp ứng tất cả các yêu cầu về nội dung và biểu thị của chứng cứ.

14.1.5 ATE_COV.2. Phân tích tổng quát

Các phụ thuộc: ADV_FSP.2 Đặc tả chức năng thực thi an toàn

ADV_FUN.1 Kiểm thử chức năng.

14.1.5.1 Mục tiêu

Mục tiêu của thành phần này là xác nhận rằng tất cả các TSFI đã được kiểm thử.

14.1.5.2 Chú thích ứng dụng

Trong thành phần này, nhà phát triển xác nhận rằng các kiểm thử trong tài liệu kiểm thử tương ứng với tất cả các TSFI trong đặc tả chức năng. Điều này có thể đạt được qua một khai báo tương ứng, có thể sử dụng một bảng, tuy nhiên nhà phát triển cũng đưa ra bản phân tích tổng quan kiểm thử.

14.1.5.3 Phần tử hành động của nhà phát triển

14.1.5.3.1 ATE_COV.2.1D

Nhà phát triển cần cung cấp bản **phân tích** tổng quan kiểm thử.

14.1.5.4 Các phần tử nội dung và trình bày

14.1.5.4.1 ATE_COV.2.1C

Bản **phân tích** tổng quan kiểm thử cần **chỉ ra** sự tương ứng giữa các kiểm thử trong tài liệu kiểm thử và các TSFI trong đặc tả chức năng.

14.1.5.4.2 ATE_COV.2.2C

Bản phân tích tổng quan kiểm thử cần minh chứng rằng tất cả các TSFI trong đặc tả chức năng đã được kiểm thử.

14.1.5.5 Phần tử hành động của đánh giá viên

14.1.5.5.1 ATE_COV.2.1E

Đánh giá viên cần xác nhận rằng thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của chứng cứ.

14.1.6 ATE_COV.3. Phân tích tổng quát chặt chẽ

Các phụ thuộc: ADV_FSP.2 Đặc tả chức năng thực thi an toàn

ADV_FUN.1 Kiểm thử chức năng

14.1.6.1 Mục tiêu

Trong phần này, mục tiêu là xác nhận rằng nhà phát triển sản phẩm đã thực hiện các kiểm thử một cách toàn diện về tất cả những cái chung trong đặc tả chức năng.

Mục tiêu của phần này là xác nhận rằng toàn bộ tham số trong tất cả các TSFI đã được kiểm thử.

14.1.6.2 Chú thích ứng dụng

Ở phần này, nhà phát triển sản phẩm được yêu cầu chỉ ra xem các kiểm thử trong tài kiểm thử tương ứng với tất cả các TSFI trong đặc tả chức năng như thế nào. Điều này có thể được thực hiện bởi một khai báo tương ứng, cũng có thể sử dụng một bảng, ngoài ra, nhà phát triển sản phẩm được yêu cầu chứng minh rằng các kiểm thử sử dụng toàn bộ các tham số của tất các TSFI. Yêu cầu bổ sung này bao gồm việc kiểm thử giới hạn và kiểm thử phủ nhận. Kiểu kiểm thử này là không thấu đáo (toàn diện) bởi vì không phải mọi giá trị có thể của tham số đều mong muốn được kiểm tra.

14.1.6.3 Phần tử hành động của nhà phát triển

14.1.6.3.1 ATE_COV.3.1D

Nhà phát triển sản phẩm cần đưa ra bản phân tích tổng quan kiểm thử

14.1.6.4 Các phần tử nội dung và trình bày

14.1.6.4.1 ATE_COV.3.1C

Bản phân tích tổng quan kiểm thử cần đưa ra sự tương đương giữa các kiểm thử trong tài liệu kiểm thử và các TSFI trong đặc tả chức năng.

14.1.6.4.2 ATE_COV.3.2C

Bản phân tích tổng quan kiểm thử cần chỉ ra rằng tất cả các TSFI trong đặc tả chức năng đã được kiểm thử **một cách hoàn chỉnh**.

14.1.6.5 Phần tử hành động của đánh giá viên

14.1.6.5.1 ATE_COV.3.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.2 Chuyên sâu (ATE_DPT)

14.2.1 Mục tiêu

Các thành phần trong họ này đề cập đến mức chi tiết mà TSF được kiểm thử bởi nhà phát triển. Việc kiểm thử TSF dựa vào các thông tin chuyên sâu nhận được từ các biểu diễn thiết kế bổ sung và các mô tả.

Mục đích là nhằm tính đến các nguy cơ bỏ qua một số lỗi trong giai đoạn triển khai TOE. Việc kiểm thử cho các giao diện đối nội chuyên biệt không những chỉ cung cấp sự đảm bảo cho các hành vi mong muốn vĩ mô như đã thể hiện trong TSF, mà còn đảm bảo các hành vi liên quan đến các cơ chế hoạt đông bên trong.

14.2.2 Phân mức thành phần

Các thành phần trong nhóm kiểm thử này được phân theo cấp độ dựa trên cơ sở của mức độ chi tiết có được trong các miêu tả TSF, từ thiết kế TOE đến miêu tả thực thi. Các cấp độ này phản ánh các miêu tả của TSF thể hiện trong lớp ADV.

14.2.3 Chú thích ứng dụng

Thiết kế TOE mô tả các thành phần bên trong ("các hệ thống thành phần" - subsystems) và có thể là các modul của TSF, cùng với sự mô tả về giao diện giữa các thành phần này và các mô đun. Chứng cứ của việc kiểm thử thiết kế TOE này cần phải chỉ ra rằng các giao diện bên trong đều đã qua kiểm

thử và bảo đảm rằng nó vận hành như đã mô tả. Điều này có thể được thực hiện bằng cách tiến hành các kiểm thử liên quan đến các giao diện ngoài của TSF, hoặc kiểm thử "hệ thống thành phần" TOE hoặc các giao diện mô đun một cách biệt lập. Quá trình kiểm thử các giao diện bên trong có thể được tiến hành theo các cách thức trực tiếp hoặc gián tiếp. Trong trường hợp chậm trễ, thiết kế TOE cần đủ chi tiết để có thể hỗ trợ triển khai các kiểm thử trực tiếp.

Trong trường hợp ở phần mô tả tinh đúng đắn về mặt kiến trúc của TSF có trích dẫn các cơ chế đặc biệt, thì các kiểm thử đã thực hiện bởi nhà phát triển sản phẩm cần phải chỉ ra rằng các cơ chế đều đã qua kiểm thử và bảo đảm rằng nó vận hành như đã mô tả.

Tại thành phần cao nhất của nhóm này, việc kiểm thử được thực hiện không chỉ theo thiết kế TOE mà còn theo sự mô tả thực thi.

14.2.4 ATE_DEPT. 1 Kiểm thử: thiết kế cơ bản

Các phụ thuộc: ADV_ARC.1 Mô tả kiến trúc an toàn

ADV_TDS.2 Thiết kế kiến trúc

ATE_FUN.1 Kiểm thử chức năng

14.2.4.1 Mục tiêu

Các mô tả "hệ thống thành phần" của một TSF cung cấp sự mô tả ở mức độ cao về các quá trình vận hành nội tại của TSF. Việc kiểm thử ở cấp độ này của "các hệ thống thành phần" TOE nhằm đảm bảo rằng "các hệ thống thành phần" của một TSF vận hành và tác động lẫn nhau như đã được mô tả trong thiết kế TOE và mô tả kiến trúc an toàn.

14.2.4.2 Phần tử hành động của nhà phát triển

14.2.4.2.1 ATE_DPT.1.1D

Nhà phát triển sản phẩm cần trình ra được bản phân tich chuyên sâu của các kiểm thử đã tiến hành.

14.2.4.3 Các phần từ nội dung và trình bày

14.2.4.3.1 ATE_DPT.1.1C

Bản phân tích chuyên sâu cần chỉ ra sự tương ứng giữa các kiểm thử trong tài liệu kiểm thử và "các hệ thống thành phần" trong thiết kế TOE.

14.2.4.3.2 ATE_DPT.1.2C

Bản phân tích chuyên sâu cần chỉ ra rằng tất cả "các hệ thống thành phần" trong thiết kế TOE đã được kiểm thử.

14.2.4.4 Phần tử hành động của đánh giá viên

14.2.4.4.1 ATE_DTP.1.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.2.5 ATE_DPT. 2 Kiểm thử: các mô đun thực thi an toàn

Các phụ thuộc: ADV_ARC.1 Mô tả kiến trúc an toàn

ADV_TDS.3 Thiết kế mang tính mô đun cơ bản

ATE_FUN.1 Kiểm thử chức năng

14.2.5.1 Mục tiêu

"Hệ thống thành phần" và các mô tả mô đun của một TSF cung cấp sự mô tả ở mức độ cao về các quá trình vận hành nội tại của TSF, và sự mô tả các giao diện của các mô đun thực thi SFR của TSF. Việc kiểm thử ở cấp độ này của mô tả TOE nhằm đảm bảo rằng "các hệ thống thành phần" của một TSF và các mô đun thực thi SFR vận hành và tác động lẫn nhau như đã được mô tả trong thiết kế TOE và mô tả kiến trúc an toàn.

14.2.5.2 Phần tử hành động của nhà phát triển

14.2.5.2.1 ATE_DPT.2.1D

Nhà phát triển sản phẩm cần trình ra được bản phân tích về mức độ chi tiết (chuyên sâu) các kiểm thử đã tiến hành.

14.2.5.3 Các phần tử nội dung và trình bày

14.2.5.3.1 ATE_DPT.2.1C

Bản phân tích chuyên sâu cần chỉ ra được sự tương ứng giữa các kiểm thử trong tài liệu kiểm thử và "các hệ thống thành phần" TSF và **các mô đun thực thi SFR** trong thiết kế TOE.

14.2.5.3.2 ATE_DPT.2.2C

Bản phân tích chuyên sâu của các kiểm thử đã tiến hành cần chỉ ra rằng "các hệ thống thành phần" TSF trong thiết kế TOE đã được kiểm thử.

14.2.5.3.3 ATE_DPT.2.3C

Bản phân tích chuyên sâu của các kiểm thử đã tiến hành cần chỉ ra rằng các mô đun thực thi SFR trong thiết kế TOE đã được kiểm thử.

14.2.5.4 Phần tử hành động của đánh giá viên

14.2.5.4.1 ATE_DPT.2.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.2.6 ATE_DEPT. 3 Kiểm thử: Thiết kế mang tính mô đun

Các phụ thuộc: ADV_ARC.1 Mô tả kiến trúc an toàn.

ADV_TDS.4 Thiết kế mang tính mô đun nửa chính thức

ATE_FUN.1 Kiểm thử chức năng

14.2.6.1 Mục tiêu

"Các hệ thống thành phần" và các mô tả mô đun của một TSF đưa ra sự mô tả mức cao quá trình vận hành nội tại của TSF và sự mô tả các giao diện của các mô đun của TSF. Việc kiểm thử ở cấp độ này của mô tả TOE nhằm đảm bảo rằng "các hệ thống thành phần" TSF và các mô đun vận hành và tác động lẫn nhau như đã được mô tả trong thiết kế TOE và mô tả kiến trúc an toàn.

14.2.6.2 Phần tử hành động của nhà phát triển

14.2.6.2.1 ATE_DPT.3.1D

Nhà phát triển sản phẩm cần trình ra được bản phân tích chuyên sâu các kiểm thử đã tiến hành.

14.2.6.3 Các phần tử nội dung và trình bày

14.2.6.3.1 ATE_DPT.3.1C

Bản phân tích chuyên sâu của việc kiểm thử cần chỉ ra sự tương ứng giữa các kiểm thử trong tài liệu kiểm thử và "các hệ thống thành phần" TSF và các mô đun trong thiết kế.

14.2.6.3.2 ATE_DPT.3.2C

Bản phân tích chuyên sâu của việc kiểm thử cần chỉ ra rằng tất cả "các hệ thống thành phần" TSF trong thiết kế TOE đã được kiểm thử.

14.2.6.3.3 ATE_DPT.3.3C

Bản phân tích chuyên sâu của việc kiểm thử cần chỉ ra rằng tất cả các mô đun TSF trong thiết kế TOE đã được kiểm thử.

14.2.6.4 Phần tử hành động của đánh giá viên

14.2.6.4.1 ATE_DTP.3.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.2.7 ATE_DPT. 4 Kiểm thử: Biểu diễn thực thi

Các phụ thuộc: ADV_ARC.1 Mô tả kiến trúc an toàn.

ADV_TDS.4 Thiết kế mang tính mô đun nửa chính thức

ADV_IMP.1 Sự thực thi của TSF

ATE_FUN.1 Kiểm thử chức năng

14.2.7.1 Mục tiêu

"Hệ thống thành phần" và các mô tả mô đun của một TSF đưa ra sự mô tả mức cao quá trình vận hành nội tại của TSF và sự mô tả các giao diện của các mô đun của TSF. Việc kiểm thử ở cấp độ này của mô tả TOE nhằm đảm bảo rằng "các hệ thống thành phần" TSF và các mô đun vận hành và tác động lẫn nhau như đã được mô tả trong thiết kế TOE và mô tả kiến trúc an toàn, và theo đúng biểu diễn thực thi.

14.2.7.2 Phần tử hành động của nhà phát triển

14.2.7.2.1 ATE_DPT.4.1D

Nhà phát triển sản phẩm cần trình ra được bản phân tích chuyên sâu các kiểm thử đã tiến hành.

14.2.7.3 Các phần tử nội dung và trình bày

14.2.7.3.1 ATE_DPT.4.1C

Bản phân tích chuyên sâu của việc kiểm thử cần chỉ ra sự tương ứng giữa các kiểm thử trong tài liệu kiểm thử và "các hệ thống thành phần" TSF và các mô đun trong thiết kế.

14.2.7.3.2 ATE_DPT.4.2C

Bản phân tích chuyên sâu của việc kiểm thử cần chỉ ra rằng tất cả "các hệ thống thành phần" TSF trong thiết kế TOE đã được kiểm thử.

14.2.7.3.3 ATE_DPT.4.3C

Bản phân tích chuyên sâu của việc kiểm thử cần chỉ ra rằng TSF hoạt động theo đúng như biểu diễn thực thi.

14.2.7.4 Phần tử hành động của đánh giá viên

14.2.7.4.1 ATE_DTP.4.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.3 Các kiểm thử chức năng (ATE_FUN)

14.3.1 Mục tiêu

Việc kiểm thử chức năng được các nhà phát triển sản phẩm tiến hành nhằm đảm bảo rằng các kiểm thử trong tài liệu kiểm thử được thực hiện và đưa thành tài liệu một cách đúng đắn. Sự tương ứng của các kiểm thử này với mô tả thiết kế TSF có được thông qua các họ Tổng quan (ATE-COV) và Chiều sâu (ATE-DPT).

Họ này góp phần vào việc đảm bảo rằng xác suất có các lỗi không bị phát hiện trong sản phẩm là tương đối nhỏ.

Tập hợp các loại kiểm thử bao gồm nhóm (họ/lớp): Tổng quan (ATE_COV), chuyên sâu ATE_DPT), và nhóm các kiểm thử chức năng (ATE_FUN) được sử dụng kết hợp nhằm định dạng các chứng cứ kiểm thử được nhà phát triển sản phẩm cung cấp (cùng với sản phẩm). Việc kiểm thử chức năng không phụ thuộc được thực hiện bởi đánh giá viên sản phẩm được phân loại vào nhóm "kiểm thử không phụ thuộc" (ATE_IDN).

14.3.2 Phân mức thành phần

Các thành phần thuộc nhóm kiểm thử này được phân làm 2 cấp độ. Trong đó, ở thành phần ở cấp độ cao hơn, các kiểm thử phụ thuộc kèm theo sẽ phải được phân tích cặn kẽ.

14.3.3 Chú thích ứng dụng

Các quy trình của các kiểm thử cần được tiến hành chính là các hướng dẫn nhằm sử dụng chương trình kiểm thử cũng như làm chủ các thiết bị hoặc công nghệ liên quan, bao gồm cả các vấn đề liên quan đến môi trường kiểm thử, điều kiện kiểm thử, các biến số và đánh giá số liệu... Quy trình kiểm thử cần phải chỉ ra được rằng, kết quả kiểm thử được tính toán như thế nào từ các số liệu đầu vào của các kiểm thử này.

Các kiểm thử phụ thuộc có liên quan, khi mà quá trình tiến hành các kiểm thử riêng biệt có thành công hay không phụ thuộc vào sự tồn tại các trạng thái riêng biệt đó. Ví dụ: có thể có các đòi hỏi như kiểm thử A phải được tiến hành trước khi thực hiện kiểm thử B, bởi vì trạng thái của sản phẩm được hình thành từ việc tiến hành thành công kiểm thử A là sự tiên quyết cho việc thực hiện thành công kiểm thử B. Như vậy, khi kiểm thử B hoạt động không như mong đợi , có thể liên quan đến vấn đề nào đó của kiểm thử phụ thuộc liên quan trước đó (trong trường hợp này là kiểm thử A).

14.3.4 ATE_FUN .1 Kiểm thử chức năng

Các phụ thuộc: ATE_COV.1 Chứng cứ tổng quan

14.3.4.1 Mục tiêu

Trong phần này, mục đích là các nhà phát triển sản phẩm dùng các kiểm thử trong nhóm này để thể hiện rằng các kiểm thử trong tài liệu kiểm thử đều được và đưa thành tài liệu chính xác.

14.3.4.2 Phần tử hành động của nhà phát triển

14.3.4.2.1 ATE_FUN.1.1D

Nhà phát triển sản phẩm cần thực hiện kiểm thử TSF và tập hợp các kết quả kiểm thử thành văn bản.

14.3.4.2.2 ATE_FUN.1.2D

Nhà phát triển sản phẩm cần đưa ra được các tài liệu kiểm thử.

14.3.4.3 Các phần tử nội dung và trình bày

14.3.4.3.1 ATE_FUN.1.1C

Tài liệu kiểm thử cần trình bày nhất quán **các kế hoạch kiểm thử, các kết quả kiểm thử mong muốn và các kết quả đo được thực tế.**

14.3.4.3.2 ATE_FUN.1.2C

Kế hoạch kiểm thử cần xác định các kiểm thử cần phải được tiến hành và mô tả các kịch bản cho mỗi hoạt động kiểm thử. Các kịch bản này bao gồm bất kỳ các kiểm thử phụ thuộc có trình tự nào dựa trên các kết quả của các kiểm thử khác.

14.3.4.3.3 ATE_FUN.1.3C

Các kết quả kiểm thử mong muốn cần chỉ ra các kết quả mang tính dự báo từ các kiểm thử được thực hiện thành công.

14.3.4.3.4 ATE_FUN.1.4C

Các kết quả kiểm thử thực sự cần phải phù hợp với các kết quả kiểm thử mong muốn.

14.3.4.4 Phần tử hành động của đánh giá viên

14.3.4.4.1 ATE_FUN.1.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.3.5 ATE_FUN. 2 Kiểm thử chức năng theo trình tự

Các phụ thuộc: ATE_COV.1 Chứng cứ tổng quan

14.3.5.1 Mục tiêu

Mục đích là để nhà phát triển sản phẩm chỉ ra rằng các kiểm thử trong tài liệu kiểm thử được thực hiện và đưa thành tài liệu chính xác, và đảm bảo rằng việc kiểm thử có cấu trúc giống như là để bác bỏ các minh chứng xung quanh sự đúng đắn của các giao diện đã được kiểm thử.

14.3.5.2 Chú thích ứng dụng

Mặc dù quy trình kiểm thử có thể chỉ ra các điều kiện tất yếu trong quá trình bố trí trình tự các kiểm thử phụ thuộc, các quy trình này chưa thể cho thấy một trình tự tối ưu hợp lý. Việc phân tích các quá trình tiến hành các kiểm thử phụ thuộc là một yếu tố quan trọng nhằm đánh giá tính tương đương của các quá trình kiểm thử khác nhau, bởi vì có khả năng các lỗi được giấu kỹ trong khi trình tự để tiến hành kiểm thử bị thay đổi.

14.3.5.3 Phần tử hành động của nhà phát triển

14.3.5.3.1 ATE_FUN.2.1D

Nhà phát triển sản phẩm cần thực hiện các kiểm thử liên quan đến TSF và tập hợp các kết quả kiểm thử thành văn bản.

14.3.5.3.2 ATE_FUN.2.2D

Nhà phát triển sản phẩm cần đưa ra được các tài liệu liên quan đến các kiểm thử đã tiến hành và các kết quả kiểm thử.

14.3.5.4 Các phần tử nội dung và trình bày

14.3.5.4.1 ATE_FUN.2.1C

Tài liệu kiểm thử cần trình bày đầu đủ các kế hoạch kiểm thử, các kết quả kiểm thử mong muốn và các kết quả kiểm thử thực sự.

14.3.5.4.2 ATE_FUN.2.2C

Các kế hoạch kiểm thử cần xác định các kiểm thử được thực hiện và mô tả các kịch bản cho mỗi hoạt động kiểm thử. Các kịch bản này bao gồm bất kỳ các kiểm thử phụ thuộc có trình tự nào dựa trên các kết quả của các kiểm thử khác.

14.3.5.4.3 ATE_FUN.2.3C

Các kết quả kiểm thử mong muốn chỉ ra các kết quả mang tính dự báo nếu như các kiểm thử được thực hiện thành công.

14.3.5.4.4 ATE_FUN.2.4C

Các kết quả kiểm thử thực sự cần bao gồm cả các kết quả kiểm thử mong muốn.

14.3.5.4.5 ATE_FUN.2.5C

Tài liệu kiểm thử cần phải bao gồm cả phần phân tích quy trình kiểm thử của các kiểm thử phụ thuộc theo trình tự.

14.3.5.4.6 ATE_FUN.2.6C

Tài liệu kiểm thử cần phải bao gồm cả phần phân tích quy trình kiểm thử của các kiểm thử phụ thuộc theo trình tự.

14.3.5.5 Phần tử hành động của đánh giá viên

14.3.5.5.1 ATE_FUN.2.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.4 Kiểm thử độc lập (ATE_IND)

14.4.1 Mục tiêu

Mục đích của nhóm này là dựa vào các sự đảm bảo có được trong các nhóm ATE_FUN, ATE_COV, và ATE_DPT bằng việc xác minh sự kiểm thử bởi nhà phát triển sản phẩm và thực hiện các kiểm thử bổ sung bởi đánh giá viên.

14.4.2 Phân mức thành phần

Các cấp độ được đề xuất trên cơ sở liên quan đến số lượng của các tài liệu kiểm thử bởi nhà phát triển sản phẩm, các hỗ trợ kiểm thử kèm theo và số lượng các kiểm thử của đánh giá viên.

14.4.3 Chú thích ứng dụng

Nhóm các kiểm thử này được đề cập đến một khi có sự đòi hỏi phải tiến hành các kiểm thử không phụ thuộc trong khuôn khổ TSF. Các kiểm thử chức năng không phụ thuộc có thể có hình thức là lặp lại (toàn bộ hoặc từng phần) các kiểm thử chức năng đã được các nhà phát triển sản phẩm tiến hành hoặc mở rộng phạm vi hay mức độ chuyên sâu của các kiểm thử đã được nhà phát triển sản phẩm tiến hành. Các hoạt động này là có tính bù trừ và một sự kết hợp hợp lý cần phải được tính đến cho mỗi TOE, trên cơ sở đảm bảo tính khả thi và tính bao trùm của các kết quả kiểm thử thu được, cũng như phải đảm bảo tính toàn vẹn chức năng của TSF.

Nhóm mẫu các kiểm thử được nhà phát triển sản phẩm đề xuất nhằm mục đích đưa ra sự chứng thực là nhà phát triển sản phẩm đã thực hiện chương trình các kiểm thử trên cơ sở TSF và đã thu được chính xác các kết quả chính thức. Phạm vi số lượng các mẫu được thu thập để tiến hành kiểm thử sẽ ảnh hưởng đến chi tiết, cũng như chất lượng của các kết quả các kiểm thử chức năng do nhà phát triển sản phẩm đắ đưa ra. Phía đánh giá viên cũng cần tính đến phạm vi các kiểm thử cần đề xuất thêm và cân đối lợi ích tương đối có thể thu được khi quan tâm đến cả hai lĩnh vực này của các kiểm thử không phụ thuộc. Cũng cần thừa nhận rằng, đôi khi việc lặp lại tất cả các kiểm thử của nhà phát triển sản phẩm đưa ra là mong muốn và khả thi, nhưng trong các trường hợp khác có thể là khá khó khăn và không hiệu quả. Cho nên cần hạn chế các thự nghiệm thực sự khó triển khai. Quá trình tiến hành lấy mẫu cần tập trung vào toàn bộ phổ của các kết quả thử nghệm đã thu được, hơn nữa cần bao gồm cả các kết quả thỏa mãn được những đòi hỏi của các kiểm thử chung (ATE_COV) và các kiểm thử chuyên biệt (ATE_DPT).

Cũng cần xem xét đến các cấu hình (cấu trúc) khác nhau của TOE trong quá trình tiến hành đánh giá. Đánh giá viên cũng cần cân nhắc tới khả năng sử dụng ngay các kết quả kiểm thử được cung cấp và căn cứ vào đó để lên kế hoạch cho các kiểm thử của riêng mình.

Sự thích hợp của TOE đối với các kiểm thử căn cứ vào khả năng truy cập vào TOE, và các tài liệu hỗ trợ cũng như các thông tin đòi hỏi (cũng liên quan đến các chương trình phần mềm kiểm thử hoặc các công cụ) để tiến hành kiểm thử. Sự cần thiết của các hỗ trợ đó chủ yếu là liên quan đến các kiểm thử phụ thuộc thuộc các nhóm (lớp) khác.

Ngoài ra, Sự thích hợp của TOE đối với các kiểm thử còn có thể nằm ở những lý do khác. Ví dụ, định dạng của TOE do nhà phát triển sản phẩm cung cấp không phải là phiên bản (ver-sion) mới nhất.

Thuật ngữ "*các giao diện*" chỉ các giao diện được mô tả trong đặc tả chức năng và thiết kế TOE, các tham số truyền qua các dẫn chứng đã đồng nhất trong mô tả thực thi. Tập hợp chính xác các giao diện đã sử dụng được lựa chọn qua các thành phần Tổng quan (ATE_COV) và Chiều sâu (ATE_DPT).

Các căn cứ cho một tập hợp con của TSF chú trọng tới khả năng cho phép đánh giá viên thiết kế một tập hợp các kiểm thử thích hợp, phù hợp với các mục tiêu mà đánh giá viên theo đuổi từ đầu.

14.4.4 ATE_IND.1 Kiểm thử độc lập - tuân thủ

Các phụ thuộc: ADV_FSP.1 Đặc tả chức năng cơ bản

AGD_OPE.1 Hướng dẫn thao tác người dùng.

AGD_PRE.1 Các quy trình chuẩn bị

14.4.4.1 Mục tiêu

Trong phần này, mục đích là để thể hiện rằng TOE hoạt động theo đúng mô tả thiết kế và các tài liệu hướng dẫn của nó.

14.4.4.2 Chú thích ứng dụng

Thành phần này không đề cập đến việc sử dụng các kết quả kiểm thử bởi nhà phát triển sản phẩm. Điều đó phù hợp với nơi mà các kết quả không thể có được và trong trường hợp việc kiểm thử bởi nhà phát triển sản phẩm được chấp nhận nhưng không có sự phê chuẩn. Đánh giá viên được yêu cầu lập ra và tiến hành các kiểm thử với mục đích xác nhận rằng TOE hoạt động đúng theo các mô tả thiết kế của nó, bao gồm cả đặc tả chức năng. Cách tiếp cận này là để đạt được sự tin cậy trong thao tác chỉnh sửa qua việc kiểm thử mẫu, hơn nữa để tiến hành mọi kiểm thử có thể. Phạm vi của kiểm thử được lập ra cho mục đích này là một sản phẩm phương pháp luận, và cần phải được xem xét trong phạm vi một TOE riêng biệt và sự cân nhắc của các hoạt động đánh giá khác.

14.4.4.3 Phần tử hành động của nhà phát triển

14.4.4.3.1 ATE_IND.1.1D

Nhà phát triển sản phẩm cần đưa ra TOE cho các kiểm thử này

14.4.4.4 Các phần tử nội dung và trình bày

14.4.4.4.1 ATE_IND.1.1C

TOE cần thích hợp cho kiểm thử.

14.4.4.5 Phần tử hành động của đánh giá viên

14.4.4.5.1 ATE_IND.1.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.4.4.5.2 ATE_IND.1.2E

Đánh giá viên cần kiểm thử một tập hợp con của TSF nhằm xác nhận rằng TOE hoạt động như đã được xác định ban đầu.

14.4.5 ATE_IND.2 Kiểm thử độc lập - lấy mẫu

Các phụ thuộc: ADV_FSP.2 Mô tả chức năng thực thi an toàn

AGD_OPE.1 Hướng dẫn thao tác người sử dụng

AGD_PRE.1 Các quy trình chuẩn bị

ATE_COV.1 Chứng cứ tổng quan

ATE_FUN.1 Kiểm thử chức năng

14.4.5.1 Mục tiêu

Trong phần này, mục đích là để thể hiện rằng TOE hoạt động đúng theo các mô tả thiết kế và các tài liệu hướng dẫn của nó. Việc kiểm thử bởi đánh giá viên xác nhận rằng nhà phát triển sản phẩm đã thực hiện một số kiểm thử của một vài giao diện trong đặc tả chức năng.

14.4.5.2 Chú thích ứng dụng

Điểm mấu chốt ở đây là nhà phát triển sản phẩm cần phải cung cấp các tài liệu cần thiết sao cho đánh giá viên có thể tái tạo lại các kiểm thử đã được tiến hành bởi nhà phát triển sản phẩm, trong đó có thể bao gồm các tài liệu kiểm thử mà máy đọc được, các chương trình (phần mềm) kiểm thử, v.v...

Đánh giá viên phải có được các kết quả (số liệu) kiểm thử từ nhà phát triển sản phẩm để hỗ trợ chương trình kiểm thử của mình. Nhá đánh giá sẽ lặp lại một loạt (mẫu) các kiểm thử của nhà phát triển sản phẩm nhằm thu được sự tin chắc vào các kết quả nhận được. Trên cơ sở có được, đánh giá viên sẽ tiến hành thêm các kiểm thử cho phép sử dụng TOE theo các cách khác, sau đó đánh giá viên sẽ tập trung kiểm thử ở những khu vực quan tâm riêng.

14.4.5.3 Phần tử hành động của nhà phát triển

14.4.5.3.1 ATE_IND.2.1D

Nhà phát triển sản phẩm cần đưa ra TOE cho các kiểm thử này.

14.4.5.4 Các phần tử nội dung và trình bày

14.4.5.4.1 ATE_IND.2.1C

TOE cần thích hợp cho kiểm thử.

14.4.5.4.2 ATE_IND.2.2C

Nhà phát triển sản phẩm cần phải đưa ra được một tập hợp các nguồn gốc tương thích với các kiểm thử chức năng đã được họ tiến hành đối với TSF.

14.4.5.5 Phần tử hành động của đánh giá viên

14.4.5.5.1 ATE_IND.2.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.4.5.5.2 ATE_IND.2.2E

Đánh giá viên cần thực hiện một bộ mẫu trong phạm vi các kiểm thử được mô tả trong tài liệu kiểm thử nhằm thẩm định các kết quả kiểm thử có được từ các nhà phát triển sản phẩm.

14.4.5.5.3 ATE_IND.2.3E

Đánh giá viên cần kiểm thử một tập hợp con thích hợp của TSF nhằm xác nhận rằng TSF hoạt động như đã được xác định ban đầu.

14.4.6 ATE_IND.3 Kiểm thử độc lập - toàn diện

Các phụ thuộc: ADV_FSP.4 Đặc tả chức năng toàn diện

AGD_OPE.1 Hướng dẫn thao tác người sử dụng

AGD_PRE.1 Các quy trình chuẩn bị

ATE_COV.1 Chứng cứ tổng quan

ATE_FUN.1 Kiểm thử chức năng

14.4.6.1 Mục tiêu

Trong phần này, mục đích là để thể hiện rằng TOE hoạt động đúng theo các mô tả thiết kế và các tài liệu hướng dẫn của nó. Việc kiểm thử bởi đánh giá viên bao gồm cả việc lặp lại toàn bộ các kiểm thử do nhà phát triển sản phẩm đã tiến hành.

14.4.6.2 Chú thích ứng dụng

Điểm mấu chốt ở đây là nhà phát triển sản phẩm cần phải cung cấp các tài liệu cần thiết sao cho đánh giá viên có thể tái tạo lại các kiểm thử đã được tiến hành bởi nhà phát triển sản phẩm, trong đó có thể bao gồm các tài liệu kiểm thử mà máy đọc được, các chương trình (phần mềm) kiểm thử, v.v...

Đánh giá viên phải có lặp lại tất cả các kiểm thử của nhà phát triển sản phẩm như là một phần trong chương trình kiểm thử của mình. Đánh giá viên sẽ lặp lại một loạt (mẫu) các kiểm thử của nhà phát triển sản phẩm nhằm thu được sự tin chắc vào các kết quả nhận được. Trên cơ sở có được, đánh giá viên sẽ tiến hành thêm các kiểm thử cho phép sử dụng TOE theo các cách khác so với cách thông thường mà nhà phát triển sản phẩm trình bày. Trừ trường hợp các kiểm thử của nhà phát triển sản phẩm tỏ ra là đã thấu đáo.

14.4.6.3 Phần tử hành động của nhà phát triển

14.4.6.3.1 ATE_IND.3.1D

Nhà phát triển sản phẩm cần đưa ra TOE cho các kiểm thử.

14.4.6.4 Các phần tử nội dung và trình bày

14.4.6.4.1 ATE_IND.3.1C

TOE cần thích hợp cho kiểm thử.

14.4.6.4.2 ATE_IND.3.2C

Nhà phát triển sản phẩm cần phải đưa ra được một tập hợp các nguồn gốc tương thích với các kiểm thử chức năng đã được họ tiến hành đối với TSF.

14.4.6.5 Phần tử hành động của đánh giá viên

14.4.6.5.1 ATE_IND.3.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

14.4.6.5.2 ATE_IND.3.2E

Đánh giá viên cần thực hiện **toàn bộ các kiểm thử** được mô tả trong tài liệu kiểm thử nhằm thẩm định các kết quả kiểm thử có được từ các nhà phát triển sản phẩm.

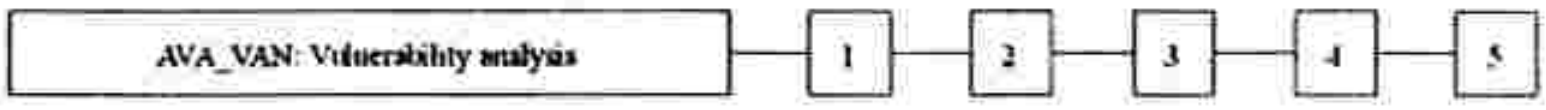
14.4.6.5.3 ATE_IND.3.3E

Đánh giá viên cần kiểm thử TSF nhằm xác nhận rằng toàn bộ TSF hoạt động như đã được xác định ban đầu.

15 Lớp AVA: Đánh giá điểm yếu

Lớp này đề cập đến khả năng khai thác các điểm yếu được giới thiệu trong quá trình phát triển.

Hình sau thể hiện các họ trong lớp này, và phân cấp các thành phần trong các họ.



Hình 15 - Phân cấp lớp AVA: Đánh giá điểm yếu

15.1 Chú thích ứng dụng

Nhìn chung, hoạt động đánh giá điểm yếu xuyên suốt các điểm yếu khác nhau trong phát triển và hoạt động của TOE. Các điểm yếu trong phát triển lợi dụng một số đặc tính của TOE được giới thiệu trong quá trình phát triển nó, như hủy bỏ tự bảo vệ của TSF thông qua việc giả mạo, trực tiếp tấn công hoặc giám sát TSF, hủy bỏ phân vùng TSF qua giám sát hoặc tấn công trực tiếp TSF, hoặc hủy bỏ không cần mật khẩu qua việc phá hủy (bằng mật khẩu) TSF. Các điểm yếu trong hoạt động lợi dụng các nhược điểm của các biện pháp phòng chống không mang tính kỹ thuật để vi phạm TOE SFR, như lạm dụng hoặc cấu hình không đúng. Lạm dụng nhằm kiểm tra xem TOE có thể được cấu hình hoặc sử dụng theo cách không an toàn mà người quản trị hoặc người dùng TOE vẫn tin rằng nó an toàn.

Việc đánh giá các điểm yếu trong phát triển được nêu trong họ đảm bảo AVA_VAN. Về cơ bản, tất cả các điểm yếu trong phát triển đều có thể được xem xét liên quan trong thành phần AVA_VAN bởi vì thực tế họ này cho phép ứng dụng với nhiều hệ phương pháp đánh giá không đặc trưng cho một kịch bản tấn công nào. Các hệ phương pháp đánh giá không đặc trưng này bao gồm cả các hệ phương pháp đặc trưng cho các TSF đó, trong đó xem xét đến các kênh trái phép (ước lượng dung lượng kênh có thể thực hiện bằng các phép đo kỹ thuật không chính thức, và các phép đo kiểm tra thực tế) hoặc có thể khắc phục bằng việc sử dụng nguồn tài nguyên đầy đủ theo hình thức tấn công trực tiếp (mô hình kỹ thuật nền tảng của các TSF này dự trên các cơ chế xác suất hoặc hoán vị; cải thiện hoạt động an toàn của chúng và các biện pháp khắc phục có thể thực hiện thông qua phân tích xác suất hay định lượng).

Nếu có các mục tiêu an toàn đã chỉ rõ trong ST để ngăn chặn sự theo dõi của một người dùng TOE khỏi người dùng khác, hoặc để đảm bảo rằng các luồng thông tin không thể được sử dụng để thu lại các tín hiệu dữ liệu trái phép đã thực thi, thì phân tích kênh trái phép cần được xét đến trong suốt quá trình tiến hành phân tích điểm yếu. Điều này thường được phản ánh trong Khả năng ẩn dấu (FPR_UNO) của TCVN 8709-2 và các chính sách kiểm soát truy cập nhiều mức đã chỉ ra thông qua chính sách kiểm soát truy cập (FDP_ACC) trong 15408-2 và/hoặc các yêu cầu chính sách kiểm soát luồng thông tin (FDP_IFC) trong ST trong 15408-2.

15.2 Phân tích điểm yếu (AVA_VAN)

15.2.1 Mục tiêu

Phân tích điểm yếu là đánh giá xem các điểm yếu tiềm ẩn được xác định trong quá trình đánh giá, trong hoạt động đoán trước được của TOE hoặc bằng các phương thức khác (ví dụ như các giả thuyết sai, các phân tích định lượng hay thống kê về hoạt động an toàn của các cơ chế an toàn đang xét) có thể cho phép những kẻ tấn công vi phạm các SFR hay không.

Phân tích điểm yếu đề cập đến các mối đe dọa do kẻ tấn công có thể phát hiện các chỗ sơ hở cho phép truy cập trái phép dữ liệu và chức năng, cho phép can thiệp hoặc sửa đổi TSF, hoặc can thiệp các quyền của các người sử dụng khác.

15.2.2 Phân mức thành phần

Phân mức thành phần dựa trên độ phức tạp tăng dần của phân tích điểm yếu thực hiện bởi đánh giá viên và mức độ tăng của khả năng tấn công gây ra bởi một kẻ tấn công để xác định và khai thác các điểm yếu tiềm ẩn.

15.2.3 AVA_VAN.1 Tổng quan điểm yếu

Các phụ thuộc:

ADV_FSP.1 Đặc tả chức năng cơ bản

AGD_OPE.1 Hướng dẫn người dùng vận hành

AGD_PRE.1 Các thủ tục chuẩn bị

15.2.3.1 Mục tiêu

Khảo sát điểm yếu của thông tin có sẵn thông báo công khai được thực hiện bởi đánh giá viên để xác định các điểm yếu tiềm ẩn có thể dễ dàng bị một kẻ tấn công tìm ra.

Đánh giá viên thực hiện việc kiểm thử xâm nhập để xác nhận rằng các điểm yếu tiềm ẩn không thể bị khai thác trong môi trường vận hành TOE. Kiểm thử xâm nhập được thực hiện bởi đánh giá viên giả thiết khả năng tấn công ở mức cơ bản.

15.2.3.2 Phần tử hành động của nhà phát triển

15.2.3.2.1 AVA_VAN.1.1D

Nhà phát triển sản phẩm cần đưa ra TOE cho các kiểm thử này.

15.2.3.3 Các phần tử nội dung và trình bày

15.2.3.3.1 AVA_VAN1.1C

TOE cần thích hợp cho kiểm thử.

15.2.3.4 Phần tử hành động của đánh giá viên

15.2.3.4.1 AVA_VAN.1.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

15.2.3.4.2 AVA_VAN.1.2E

Đánh giá viên cần thực hiện việc tìm kiếm các nguồn thông tin công cộng để nhận biết các điểm yếu tiềm ẩn trong TOE

15.2.3.4.3 AVA_VAN.1.3E

Đánh giá viên cần tiến hành việc kiểm thử xâm nhập dựa trên các điểm yếu tiềm ẩn đã biết để xác nhận rằng TOE được bảo vệ trước các tấn công của kẻ tấn công với khả năng tấn công cơ bản.

15.2.4 AVA_VAN.2 Phân tích điểm yếu

Các phụ thuộc: ADV_ARC.1 Mô tả kiến trúc an toàn.

ADV_FSP.1 Đặc tả chức năng cơ bản

ADV_TDS.1 Thiết kế cơ bản

AGD_OPE.1 Hướng dẫn người dùng vận hành

AGD_PRE.1 Các thủ tục chuẩn bị

15.2.4.1 Mục tiêu

Phân tích điểm yếu được thực hiện bởi đánh giá viên nhằm xác định chắc chắn sự có mặt của các điểm yếu tiềm ẩn.

Đánh giá viên thực hiện việc kiểm thử xâm nhập để xác nhận rằng các điểm yếu tiềm ẩn không thể bị khai thác trong môi trường vận hành TOE. Kiểm thử xâm nhập được thực hiện bởi đánh giá viên áp dụng khả năng tấn công ở mức cơ bản.

15.2.4.2 Phần tử hành động của nhà phát triển

15.2.4.2.1 AVA_VAN.2.1D

Nhà phát triển cần cung cấp TOE để kiểm thử.

15.2.4.3 Các phần tử nội dung và trình bày

15.2.4.3.1 AVA_VAN.2.1C

TOE cần thích hợp cho kiểm thử.

15.2.4.4 Phần tử hành động của đánh giá viên

15.2.4.4.1 AVA_VAN.2.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

15.2.4.4.2 AVA_VAN.2.2E

Đánh giá viên cần thực hiện việc tìm kiếm các nguồn thông tin công cộng để nhận biết các điểm yếu tiềm ẩn trong TOE.

15.2.4.4.3 AVA_VAN.2.3E

Đánh giá viên cần thực hiện phân tích điểm yếu độc lập của TOE thông qua tài liệu hướng dẫn, đặc tả chức năng, thiết kế TOE và mô tả kiến trúc an toàn để xác định các điểm yếu tiềm ẩn trong TOE.

15.2.4.4.4 AVA_VAN.2.4E

Đánh giá viên cần tiến hành việc kiểm thử xâm nhập dựa trên các điểm yếu tiềm ẩn đã biết để xác nhận rằng TOE được bảo vệ các tấn công của kẻ tấn công với khả năng tấn công cơ bản.

15.2.5 AVA_VAN.3 Phân tích các điểm yếu trọng tâm

Các phụ thuộc: ADV_ARC.1 Mô tả kiến trúc an toàn

ADV_FSP.2 Đặc tả chức năng thực thi an toàn

ADV_TDS.3 Thiết kế mô đun cơ bản

ADV_TMP.1 Biểu diễn triển khai của TSF

AGD_OPE.1 Hướng dẫn người dùng vận hành

AGD_PRE.1 Các thủ tục chuẩn bị

15.2.5.1 Mục tiêu

Phân tích điểm yếu được thực hiện bởi đánh giá viên nhằm xác định chắc chắn sự có mặt của các điểm yếu tiềm ẩn.

Đánh giá viên thực hiện việc kiểm thử xâm nhập để xác nhận rằng các điểm yếu tiềm ẩn không thể bị khai thác trong môi trường vận hành TOE. Kiểm thử xâm nhập được thực hiện bởi đánh giá viên áp dụng khả năng tấn công ở mức cơ bản nâng cao.

15.2.5.2 Phần tử hành động của nhà phát triển

15.2.5.2.1 AVA_VAN.3.1D

Nhà phát triển cần cung cấp TOE cho kiểm thử.

15.2.5.3 Các phần tử nội dung và trình bày

15.2.5.3.1 AVA_VAN.3.1C

TOE cần thích hợp cho kiểm thử.

15.2.5.4 Phần tử hành động của đánh giá viên

15.2.5.4.1 AVA_VAN.3.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

15.2.5.4.2 AVA_VAN.3.2E

Đánh giá viên cần thực hiện việc tìm kiếm các nguồn thông tin công cộng để nhận biết các điểm yếu tiềm ẩn trong TOE.

15.2.5.4.3 AVA_VAN.3.3E

Đánh giá viên cần thực hiện phân tích điểm yếu độc lập của TOE thông qua tài liệu hướng dẫn, đặc tả chức năng, thiết kế TOE và mô tả kiến trúc an toàn **và biểu diễn triển khai** để xác định các điểm yếu tiềm ẩn trong TOE.

15.2.5.4.4 AVA_VAN.3.4E

Đánh giá viên cần tiến hành việc kiểm thử xâm nhập dựa trên các điểm yếu tiềm ẩn đã biết để xác nhận rằng TOE được bảo vệ trước các tấn công của kẻ tấn công với khả năng tấn công **cơ bản nâng cao**.

15.2.6 AVA_VAN.4 Phân tích điểm yếu có hệ thống

Các phụ thuộc: ADV_ARC.1 Mô tả kiến trúc an toàn

ADV_FSP.2 Đặc tả chức năng thực thi an toàn

ADV_TDS.3 Thiết kế mô đun cơ bản

ADV_TMP.1 Biểu diễn triển khai của TSF

AGD_OPE.1 Hướng dẫn người dùng vận hành

AGD_PRE.1 Các thủ tục chuẩn bị

15.2.6.1 Mục tiêu

Phân tích điểm yếu có hệ thống được thực hiện bởi đánh giá viên nhằm xác định chắc chắn sự có mặt của các điểm yếu tiềm ẩn.

Đánh giá viên thực hiện việc kiểm thử xâm nhập để xác nhận rằng các điểm yếu tiềm ẩn không thể bị khai thác trong môi trường vận hành TOE. Kiểm thử xâm nhập được thực hiện bởi đánh giá viên áp dụng khả năng tấn công ở mức vừa phải.

15.2.6.2 Phần tử hành động của nhà phát triển

15.2.6.2.1 AVA_VAN.4.1D

Nhà phát triển cần cung cấp TOE cho kiểm thử.

15.2.6.3 Các phần tử nội dung và trình bày

15.2.6.3.1 AVA_VAN.4.1C

TOE cần thích hợp cho kiểm thử.

15.2.6.4 Phần tử hành động của đánh giá viên

15.2.6.4.1 AVA_VAN.4.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

15.2.6.4.2 AVA_VAN.4.2E

Đánh giá viên cần thực hiện việc tìm kiếm các nguồn thông tin công cộng để nhận biết các điểm yếu tiềm ẩn trong TOE.

15.2.6.4.3 AVA_VAN.4.3E

Đánh giá viên cần thực hiện phân tích điểm yếu có hệ thống, độc lập của TOE sử dụng tài liệu hướng dẫn, đặc tả chức năng, thiết kế TOE và mô tả kiến trúc an toàn và biểu diễn triển khai để xác định các điểm yếu tiềm ẩn trong TOE.

15.2.6.4.4 AVA_VAN.4.4E

Đánh giá viên cần tiến hành việc kiểm thử xâm nhập dựa trên các điểm yếu tiềm ẩn đã biết để xác nhận rằng TOE được bảo vệ trước các tấn công của kẻ tấn công với khả năng tấn công **vừa phải**.

15.2.7 AVA_VAN.5 Phân tích điểm yếu có hệ thống nâng cao

Các phụ thuộc: ADV_ARC.1 Mô tả kiến trúc an toàn

ADV_FSP.2 Đặc tả chức năng thực thi an toàn

ADV_TDS.3 Thiết kế mô đun cơ bản

ADV_TMP.1 Biểu diễn triển khai của TSF

AGD_OPE.1 Hướng dẫn người dùng vận hành

AGD_PRE.1 Các thủ tục chuẩn bị

15.2.7.1 Mục tiêu

Phân tích điểm yếu có hệ thống được thực hiện bởi đánh giá viên nhằm xác định chắc chắn sự có mặt của các điểm yếu tiềm ẩn.

Đánh giá viên thực hiện việc kiểm thử xâm nhập để xác nhận rằng các điểm yếu tiềm ẩn không thể bị khai thác trong môi trường vận hành TOE. Kiểm thử xâm nhập được thực hiện bởi đánh giá viên áp dụng khả năng tấn công ở mức cao.

15.2.7.2 Phần tử hành động của nhà phát triển

15.2.7.2.1 AVA_VAN.5.1D

Nhà phát triển cần cung cấp TOE cho kiểm thử.

15.2.7.3 Các phần tử nội dung và trình bày

15.2.7.3.1 AVA_VAN.5.1C

TOE cần thích hợp cho kiểm thử.

15.2.7.4 Phần tử hành động của đánh giá viên

15.2.7.4.1 AVA_VAN.5.1E

Đánh giá viên cần xác nhận rằng các thông tin có được đã đạt tất cả các yêu cầu về nội dung và hình thức của các chứng cứ.

15.2.7.4.2 AVA_VAN.5.2E

Đánh giá viên cần thực hiện việc tìm kiếm thông tin công cộng để nhận biết các điểm yếu tiềm ẩn trong TOE.

15.2.7.4.3 AVA_VAN.5.3E

Đánh giá viên cần thực hiện phân tích điểm yếu có hệ thống, độc lập của TOE thông qua tài liệu hướng dẫn, đặc tả chức năng, thiết kế TOE, mô tả kiến trúc an toàn và biểu diễn triển khai để xác định các điểm yếu tiềm ẩn trong TOE.

15.2.7.4.4 AVA_VAN.5.4E

Đánh giá viên cần tiến hành việc kiểm thử xâm nhập dựa trên các điểm yếu tiềm ẩn đã biết để xác nhận rằng TOE được bảo vệ trước các tấn công của kẻ tấn công với khả năng tấn công cao.

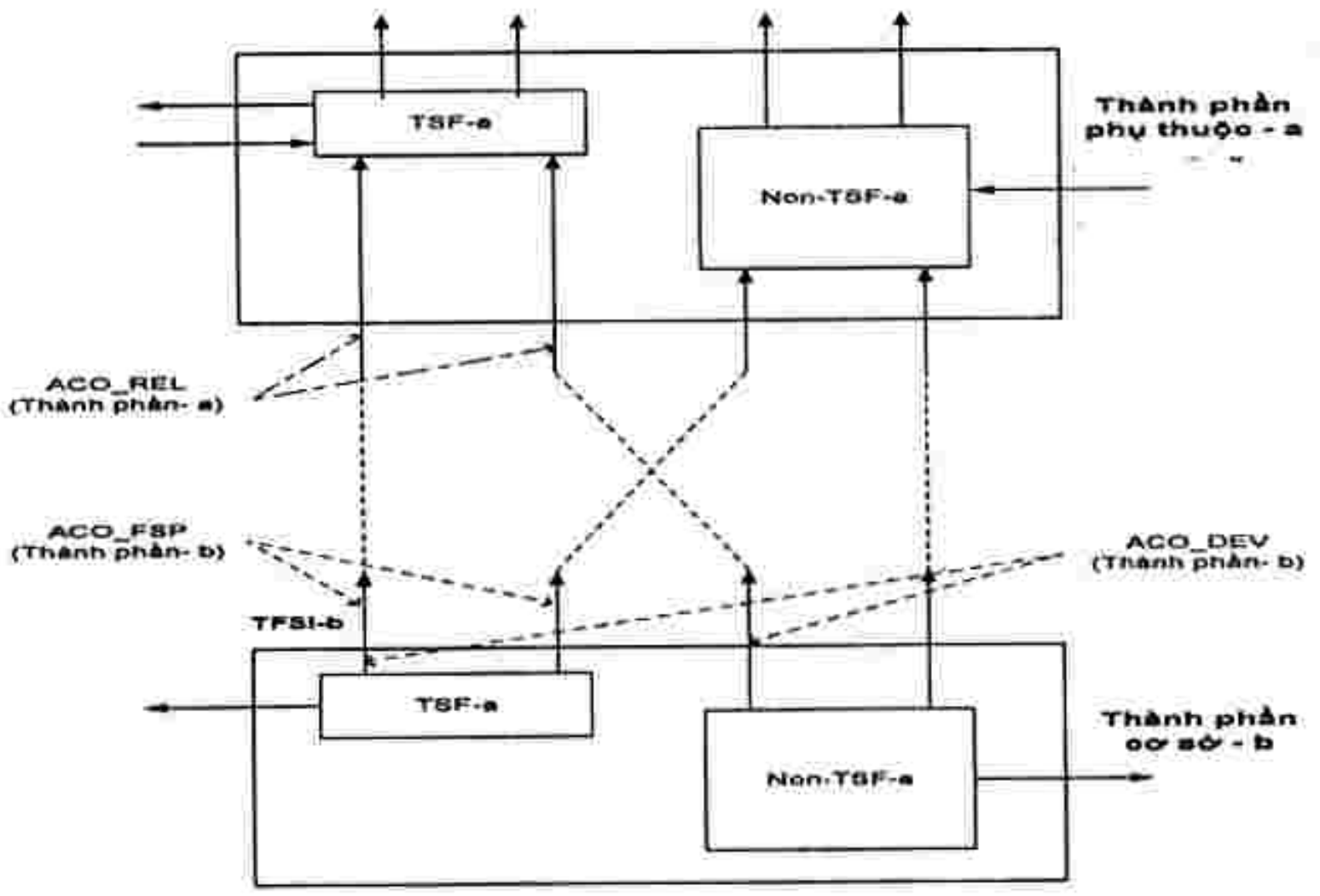
16 Lớp ACO: Tổng hợp

Lớp tổng hợp ACO bao gồm năm họ. Những họ này xác định các yêu cầu đảm bảo được thiết kế để đưa ra sự tin cậy về việc một TOE được tổng hợp sẽ hoạt động an toàn dựa vào chức năng an toàn cung cấp bởi các thành phần phần mềm, phần sụn hoặc phần cứng đã được đánh giá trước đó.

Tổng hợp là việc gộp hai hay nhiều thực thể CNTT đã được đánh giá thỏa mãn các gói yêu cầu đảm bảo an toàn trong TCVN 8709 (các thành phần cơ sở và thành phần phụ thuộc, xem Phụ lục B) và kết hợp chúng để sử dụng không cần phát triển thêm một thực thể CNTT nào khác. Việc phát triển thêm các thực thể CNTT không được xét đến (các thực thể chưa được xem xét trước đó trong đánh giá thành phần). Các TOE tổng hợp tạo thành một sản phẩm mới có thể được cài đặt và tích hợp vào bất kỳ môi trường cụ thể nào đáp ứng các mục tiêu của môi trường đánh giá.

Cách tiếp cận này không đưa ra một phương pháp thay thế cho đánh giá thành phần. Tổng hợp thuộc ACO cung cấp một phương pháp cho việc tích hợp TOE tổng hợp, phương pháp này có thể dùng thay thế cho các mức đảm bảo khác đã nêu trong TCVN 8709, nhằm đạt được sự tin cậy trong một TOE tạo thành qua kết hợp hai hay nhiều thành phần đã đánh giá tuân thủ mà không cần phải đánh giá lại TSF tổng hợp. (Người tích hợp TOE tổng hợp còn được gọi là "nhà phát triển" trong toàn bộ lớp ACO, với mọi tham chiếu đến nhà phát triển các thành phần cơ sở hoặc thành phần phụ thuộc khi được nêu rõ như vậy).

Các gói bảo đảm tổng hợp được định nghĩa tại điều khoản 8 và 6.3, là một thang bậc đảm bảo cho các TOE tổng hợp. Thang bậc đảm bảo này được đòi hỏi thêm cho EAL vì để kết hợp các thành phần đã được đánh giá theo EALs và đạt được kết quả bảo đảm theo EAL, tất cả các SAR trong EAL phải được áp dụng cho các TOE tổng hợp. Dù rằng có thể tái sử dụng các kết quả đánh giá TOE thành phần, vẫn thường cần xem xét thêm các khía cạnh khác của các thành phần của TOE tổng hợp, như đã nêu trong Phụ lục B.3. Do trong hoạt động đánh giá một TOE tổng hợp có sự tham gia của các bên khác nhau, nói chung là không thể có được mọi chứng cứ cần thiết về các khía cạnh khác của các thành phần này để áp dụng EAL phù hợp. Do đó, các CAPs được định nghĩa nhằm giải quyết vấn đề về kết hợp các thành phần đã đánh giá và nhằm đạt một kết quả có nghĩa hơn. Điều này được thảo luận thêm trong Phụ lục B.



Hình 16 - Mối quan hệ giữa các họ ACO và tương tác giữa các thành phần

Thông thường trong một TOE tổng hợp, một thành phần dựa trên các dịch vụ do thành phần khác cung cấp. Các thành phần yêu cầu dịch vụ được gọi là thành phần phụ thuộc và các thành phần cung cấp dịch vụ được gọi là thành phần cơ sở. Sự tương tác và phân biệt này được bàn thêm tại Phụ lục B. Giả thiết là nhà phát triển thành phần phụ thuộc hỗ trợ đánh giá TOE theo một số cách thức nào đó (như nhà phát triển, người tài trợ, hoặc chỉ là hợp tác và cung cấp các chứng cứ đánh giá cần thiết từ việc đánh giá thành phần phụ thuộc). Các thành phần ACO trong các gói bảo đảm CAP không được sử dụng như một sự gia tăng các đánh giá TOE thành phần, vì điều này không đem lại đảm bảo có nghĩa cho thành phần.

Các họ trong lớp ACO tương tác một cách tương tự với các lớp ADV, ATE và AVA trong đánh giá TOE thành phần và do đó có thể chịu ảnh hưởng của đặc tả các yêu cầu từ những lớp này. Tuy nhiên, có một số điều khoản đặc trưng cho đánh giá TOE tổng hợp. Để xác định cách thức các thành phần tương tác và tìm ra những sai lệch trong đánh giá các thành phần, cần xác định các mối phụ thuộc

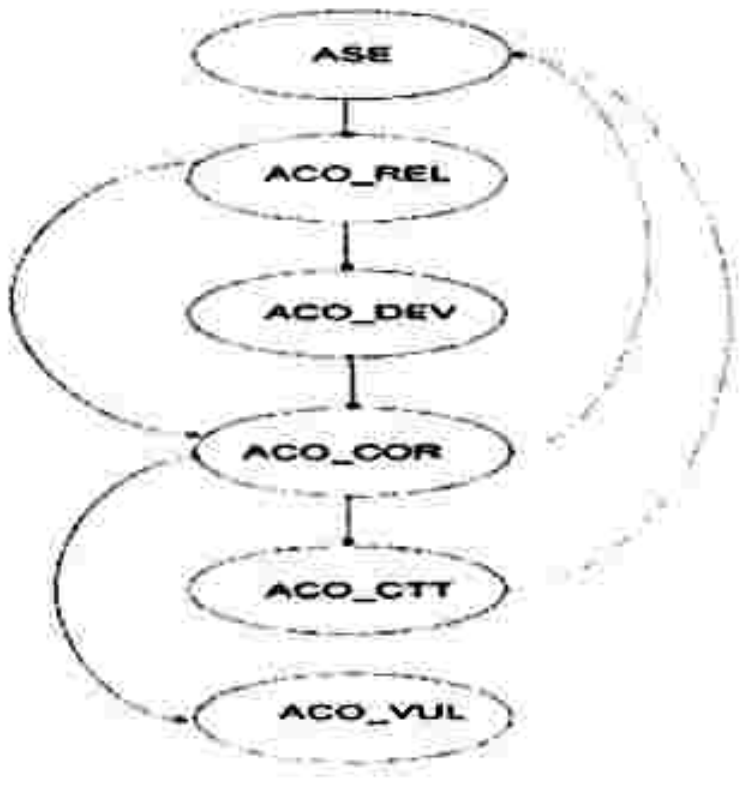
(ACO_REL) của các thành phần phụ thuộc vào các thành phần cơ sở. Các mối phụ thuộc vào thành phần cơ sở này được quy định trong điều khoản về giao diện qua đó thành phần phụ thuộc gọi các dịch vụ với sự hỗ trợ của các SFR thành phần phụ thuộc. Các giao diện, và ở mức cao hơn là các hoạt động hỗ trợ, được cung cấp bởi các thành phần cơ sở để đáp ứng những yêu cầu dịch vụ được phân tích trong ACO_DEV. Các họ ACO_DEV dựa trên họ ADV_TDS, do đó tại mức đơn giản nhất, TSF của mỗi thành phần có thể được xem như là một hệ thống con của TOE tổng hợp, với các phần bổ sung thêm cho mỗi thành phần được xem là các hệ thống con bổ sung. Vì vậy, các giao diện giữa các thành phần được xem là tương tác giữa các hệ thống con trong đánh giá TOE thành phần.

Có thể là các giao diện và mô tả hoạt động hỗ trợ cung cấp cho ACO_DEV chưa đầy đủ. Điều này được xác định trong quản lý ACO_COR. Họ ACO_COR nhận kết quả từ ACO_REL và ACO_DEV, xác định việc các thành phần đang được sử dụng trong cấu hình đánh giá của chúng hay không, và xác định vị trí đặc tả nào đó chưa đầy đủ, từ đó xác định làm yếu tố đầu vào cho các hoạt động kiểm thử (ACO_CTT) và phân tích điểm yếu (ACO_VUL) cho TOE tổng hợp.

Kiểm thử TOE tổng hợp được thực hiện để xác định rằng các TOE tổng hợp có hoạt động dự kiến như đã xác định bởi các SFRs của TOE tổng hợp và nhằm biểu diễn sự phù hợp của các giao diện giữa các thành phần của TOE tổng hợp ở các mức cao hơn.

Các phân tích điểm yếu của TOE tổng hợp có được từ những kết quả đầu ra của phân tích điểm yếu của các đánh giá thành phần. Phân tích điểm yếu TOE tổng hợp xem xét mọi điểm yếu sẵn có từ các đánh giá thành phần nhằm xác định rằng các điểm yếu đó không áp dụng cho các TOE tổng hợp. Việc tìm kiếm thông tin công bố công khai liên quan đến các thành phần cũng được thực hiện để xác định ra mọi vấn đề đã báo cáo trong các thành phần sau khi hoàn thành đánh giá tương ứng.

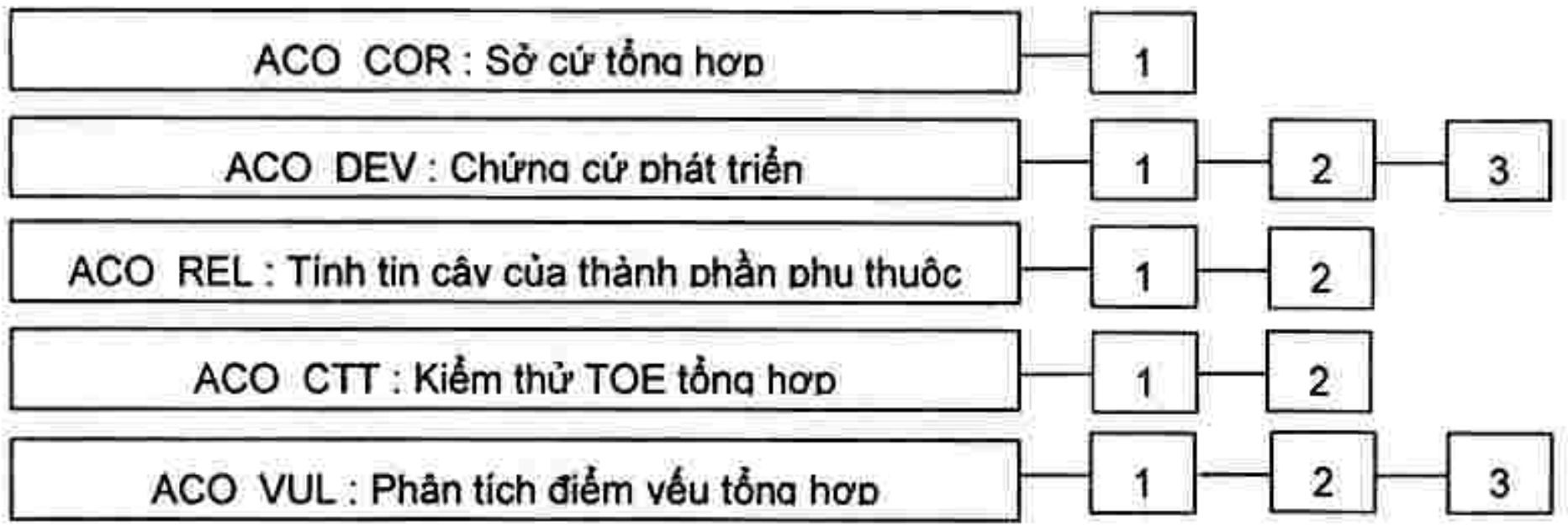
Sự tương tác giữa các họ ACO được mô tả trong Hình 17 dưới đây. Tương tác này thể hiện bằng các đường mũi tên liền nét, trong đó chứng cứ và hiểu biết về một họ được chuyển vào hoạt động tiếp theo. Các đường mũi tên đứt nét xác định dấu vết rõ ràng về một hoạt động có từ các SFR của TOE tổng hợp như mô tả ở trên.



Hình 17 - Mối quan hệ giữa các họ ACO

Thảo luận thêm về định nghĩa và tương tác trong các TOE tổng hợp được đưa ra trong Phụ lục B.

Hình 18 cho thấy các họ trong lớp này, và phân cấp các thành phần trong các họ.



Hình 18 – Phân cấp lớp ACO: Tổng hợp

16.1 Sở cứ tổng hợp (ACO_COR)

16.1.1 Mục tiêu

Họ này đề cập đến yêu cầu chứng minh rằng thành phần cơ sở có thể cung cấp một mức độ bảo đảm thích hợp để sử dụng vào việc tổng hợp.

16.1.2 Phân mức thành phần

Chỉ có một thành phần duy nhất trong họ này.

16.1.3 ACO_COR.1 Sở cứ tổng hợp

Phụ thuộc: ACO_DEV.1 Mô tả chức năng
ALC_CMC.1 Ghi nhãn cho TOE
ACO_REL.1 Thông tin tin cậy cơ bản

16.1.3.1 Phần tử hành động của nhà phát triển

16.1.3.1.1 ACO_COR.1.1D

Nhà phát triển cần cung cấp sở cứ tổng hợp cho thành phần cơ sở.

16.1.3.2 Các phần tử nội dung và trình bày

16.1.3.2.1 ACO_COR.1.1C

Sở cứ tổng hợp cần biểu thị rằng một mức bảo đảm ít nhất đạt ngang như mức của thành phần phụ thuộc đã thu được nhằm hỗ trợ chức năng thành phần cơ sở, khi thành phần cơ sở được cấu hình theo yêu cầu để hỗ trợ TSF của thành phần phụ thuộc.

16.1.3.3 Phần tử hành động của đánh giá viên

16.1.3.3.1 ACO_COR.1.1E

Đánh giá viên phải xác nhận rằng thông tin đáp ứng tất cả yêu cầu đối với nội dung và hình thức của chứng cứ.

16.2 Chứng cứ phát triển (ACO_DEV)

16.2.1 Mục tiêu

Họ này đặt ra yêu cầu về đặc tả cho thành phần cơ sở theo các mức tăng dần về chi tiết. Thông tin này cần có để đạt được sự tin cậy về việc chức năng an toàn thích hợp được đưa ra nhằm hỗ trợ yêu cầu của thành phần phụ thuộc (như đã xác định trong thông tin tin cậy).

16.2.2 Phân mức thành phần

Các thành phần được phân mức trên cơ sở tăng dần chi tiết về các giao diện đã đưa ra, cách thức chúng được triển khai.

16.2.3 Chú thích ứng dụng

TSF của thành phần cơ sở thường được xác định không cần biết đến các mối phụ thuộc của các ứng dụng có thể có khi chúng được tổng hợp. TSF của thành phần cơ sở này được định nghĩa bao gồm tất cả các phần của thành phần cơ sở dựa vào việc thực thi các SFRs của thành phần cơ sở. Điều đó cũng nghĩa là bao gồm tất cả các phần của thành phần cơ sở cần thiết để triển khai các SFRs của thành phần cơ sở.

Đặc tả chức năng của thành phần cơ sở sẽ mô tả TSFI với những điều khoản về giao diện do thành phần cơ sở đưa ra nhằm cho phép thực thể bên ngoài thực thi các hoạt động của TSF. Nó gồm giao diện với người dùng nhằm cho phép tương tác với hoạt động của TSF thực thi các SFRs và giao diện cho phép một thực thể CNTT bên ngoài tạo các lời gọi tới TSF.

Đặc tả chức năng chỉ mô tả những gì TSF đưa ra ở giao diện của nó và phương thức chức năng TSF được thực hiện. Do đó, đặc tả chức năng không cần thiết phải cung cấp một đặc tả giao diện đầy đủ cho tất cả các giao diện khả thi giữa một thực thể bên ngoài và thành phần cơ sở. Nó không bao gồm những gì TSF muốn có/ yêu cầu từ môi trường hoạt động. Mô tả về những gì một TSF thành phần phụ thuộc dựa vào một thành phần cơ sở được xem xét trong lớp Độ tin cậy của thành phần phụ thuộc (ACO_REL), và chứng cứ thông tin phát triển cung cấp phản hồi về các giao diện đã xác định.

Chứng cứ thông tin phát triển bao gồm một đặc tả thành phần cơ sở. Đó có thể là chứng cứ sử dụng trong đánh giá thành phần cơ sở nhằm thỏa mãn các yêu cầu ADV, hoặc có thể là hình thức chứng cứ khác tạo bởi hoặc nhà phát triển thành phần cơ sở hay nhà phát triển TOE tổng hợp. Đặc tả thành phần cơ sở được sử dụng trong lớp Chứng cứ phát triển (ACO_DEV) nhằm đạt được sự tin cậy về việc chức năng an toàn thích hợp được đưa ra để hỗ trợ các yêu cầu của thành phần phụ thuộc. Mức chi tiết đòi hỏi của chứng cứ này tăng dần nhằm phản ánh mức bảo đảm đã yêu cầu trong TOE tổng hợp. Điều này được mong đợi nhằm phản ánh chung về sự tin cậy tăng dần đạt được từ việc ứng dụng các gói đảm bảo cho các thành phần. Đánh giá viên xác định rằng mô tả về thành phần cơ sở này nhất quán với thông tin tin cậy đã cung cấp cho thành phần phụ thuộc.

16.2.4 ACO_DEV.1 Mô tả chức năng

Phụ thuộc: ACO_REL.1 Thông tin tin cậy cơ bản

16.2.4.1 Mục tiêu

Cần có một mô tả về các giao diện trong thành phần cơ sở làm nền tảng cho thành phần phụ thuộc. Cần kiểm tra để xác định xem nó có nhất quán với mô tả các giao diện làm nền tảng cho thành phần phụ thuộc hay không, như đã cung cấp trong thông tin tin cậy.

16.2.4.2 Phần tử hành động của nhà phát triển

16.2.4.2.1 ACO_DEV.1.1D

Nhà phát triển cần đưa ra thông tin phát triển cho thành phần cơ sở.

16.2.4.3 Các phần tử nội dung và trình bày

16.2.4.3.1 ACO_DEV.1.1C

Thông tin phát triển cần mô tả mục đích mỗi giao diện thành phần cơ sở sử dụng trong TOE tổng hợp.

16.2.4.3.2 ACO_DEV.1.2C

Thông tin phát triển cần chỉ ra sự phù hợp giữa các giao diện, sử dụng trong TOE tổng hợp, của thành phần cơ sở và thành phần phụ thuộc nhằm hỗ trợ TSF của thành phần phụ thuộc.

16.2.4.4 Phần tử hành động của đánh giá viên

16.2.4.4.1 ACO_DEV.1.1E

Đánh giá viên cần xác nhận rằng thông tin đáp ứng tất cả yêu cầu về nội dung và trình bày của chứng cứ.

16.2.4.4.2 ACO_DEV.1.2E

Đánh giá viên cần xác định rằng mô tả giao diện đã cung cấp nhất quán với thông tin tin cậy đã cung cấp cho thành phần phụ thuộc.

16.2.5 ACO_DEV.2 Chứng cứ cơ bản của thiết kế

Phụ thuộc: ACO_REL.1 Thông tin tin cậy cơ bản

16.2.5.1 Mục tiêu

Cần có một mô tả về các giao diện trong thành phần cơ sở làm nền tảng cho thành phần phụ thuộc. Cần kiểm tra để xác định xem nó có nhất quán với mô tả các giao diện làm nền tảng cho thành phần phụ thuộc hay không, như đã cung cấp trong thông tin tin cậy.

Ngoài ra, hoạt động an toàn của thành phần cơ sở có hỗ trợ thành phần phụ thuộc TSF được mô tả.

16.2.5.2 Phần tử hành động của nhà phát triển

16.2.5.2.1 ACO_DEV.2.1D

Nhà phát triển cần đưa ra thông tin phát triển cho thành phần cơ sở.

16.2.5.3 Các phần tử nội dung và trình bày

16.2.5.3.1 ACO_DEV.2.1C

Các thông tin phát triển sẽ mô tả các mục đích **và phương pháp sử dụng** của từng giao diện thành phần cơ sở được sử dụng trong TOE tổng hợp.

16.2.5.3.2 ACO_DEV.2.2C

Thông tin phát triển cần đưa ra mô tả mức cao về hoạt động của thành phần cơ sở hỗ trợ việc thực thi các SFRs của thành phần phụ thuộc.

16.2.5.3.3 ACO_DEV.2.3C

Thông tin phát triển cần chỉ ra sự phù hợp giữa các giao diện, sử dụng trong TOE tổng hợp, của thành phần cơ sở và thành phần phụ thuộc nhằm hỗ trợ TSF của thành phần phụ thuộc.

16.2.5.4 Phần tử hành động của đánh giá viên

16.2.5.4.1 ACO_DEV.2.1E

Đánh giá viên cần xác nhận rằng thông tin đáp ứng tất cả yêu cầu về nội dung và trình bày của chứng cứ.

16.2.5.4.2 ACO_DEV.2.2E

Đánh giá viên cần xác định rằng mô tả giao diện đã cung cấp nhất quán với thông tin tin cậy đã cung cấp cho thành phần phụ thuộc.

16.2.6 ACO_DEV.3 Chứng cứ chi tiết của thiết kế

Phụ thuộc: ACO_REL.2 Thông tin tin cậy

16.2.6.1 Mục tiêu

Cần có một mô tả về các giao diện trong thành phần cơ sở làm nền tảng cho thành phần phụ thuộc. Cần kiểm tra để xác định xem nó có nhất quán với mô tả các giao diện làm nền tảng cho thành phần phụ thuộc hay không, như đã cung cấp trong thông tin tin cậy.

Mô tả giao diện kiến trúc của thành phần cơ sở được cung cấp để cho phép đánh giá viên xác định giao diện này có tạo thành một phần của TSF của thành phần cơ sở hay không.

16.2.6.2 Phần tử hành động của nhà phát triển

16.2.6.2.1 ACO_DEV.3.1D

Nhà phát triển cần đưa ra thông tin phát triển cho thành phần cơ sở.

16.2.6.3 Các phần tử nội dung và trình bày

16.2.6.3.1 ACO_DEV.3.1C

Các thông tin phát triển sẽ mô tả các mục đích và phương pháp sử dụng của từng giao diện thành phần cơ sở được sử dụng trong TOE tổng hợp.

16.2.6.3.2 ACO_DEV.3.2C

Thông tin phát triển cần xác định các hệ thống con của thành phần cơ sở, cung cấp các giao diện của thành phần cơ sở dùng trong TOE tổng hợp.

16.2.6.3.3 ACO_DEV.3.3C

Thông tin phát triển cần đưa ra mô tả mức cao về hoạt động của thành phần cơ sở hỗ trợ việc thực thi các SFRs của thành phần phụ thuộc.

16.2.6.3.4 ACO_DEV.3.4C

Thông tin phát triển cần cung cấp một ánh xạ từ các giao diện tới các hệ thống con của thành phần cơ sở.

16.2.6.3.5 ACO_DEV.3.5C

Thông tin phát triển cần chỉ ra sự phù hợp giữa các giao diện, sử dụng trong TOE tổng hợp, của thành phần cơ sở và thành phần phụ thuộc nhằm hỗ trợ TSF của thành phần phụ thuộc.

16.2.6.4 Phần tử hành động của đánh giá viên

16.2.6.4.1 ACO_DEV.3.1E

Đánh giá viên cần xác nhận rằng thông tin đáp ứng tất cả yêu cầu về nội dung và trình bày của chứng cứ.

16.2.6.4.2 ACO_DEV.3.2E

Đánh giá viên cần xác định rằng mô tả giao diện đã cung cấp nhất quán với thông tin tin cậy đã cung cấp cho thành phần phụ thuộc.

16.3 Tính tin cậy của thành phần phụ thuộc (ACO_REL)

16.3.1 Mục tiêu

Mục đích của họ này là cung cấp chứng cứ mô tả sự tin cậy mà một thành phần phụ thuộc có được khi dựa vào thành phần cơ sở. Thông tin này hữu ích để người có trách nhiệm tích hợp thành phần với các thành phần CNTT đã được đánh giá khác nhằm tạo ra TOE tổng hợp, và cung cấp chi tiết về các đặc tính an toàn của sản phẩm tổng hợp.

Họ này đưa ra mô tả về giao diện giữa thành phần phụ thuộc và thành phần cơ sở của TOE tổng hợp. Giao diện này có thể không được phân tích trong đánh giá từng thành phần, vì các giao diện không phải là TSFIs của các TOE thành phần riêng lẻ.

16.3.2 Phân mức thành phần

Các thành phần trong họ này được phân mức tương ứng với số lượng chi tiết cung cấp trong mô tả về sự tin cậy của thành phần phụ thuộc vào thành phần cơ sở.

16.3.3 Chú thích ứng dụng

Họ "Sự tin cậy của thành phần phụ thuộc" (ACO_REL) xem xét tương tác giữa các thành phần, trong đó thành phần phụ thuộc dựa vào một dịch vụ của thành phần cơ sở để hỗ trợ hoạt động của chức năng an toàn của thành phần phụ thuộc. Các giao diện tới các dịch vụ này của thành phần cơ sở có thể đã không được xem xét trong đánh giá thành phần cơ sở do dịch vụ trong thành phần cơ sở đã không được xem xét tính an toàn liên quan trong đánh giá thành phần, hoặc vì mục đích kế thừa của dịch vụ (ví dụ, điều chỉnh kiểu font) hoặc bởi vì các SFRs liên quan tới TCVN 8709 đã không được yêu cầu trong ST của thành phần cơ sở (ví dụ giao diện đăng nhập khi không có yêu cầu về "FIA: các SFRs định danh và xác thực" theo TCVN 8709-2). Các giao diện tới thành phần cơ sở này thường được xem như giao diện chức năng trong đánh giá thành phần cơ sở, và xem xét thêm trong đặc tả chức năng cùng với các giao diện an toàn (TSFI).

Tóm lại, các TSFIs được mô tả trong đặc tả chức năng chỉ bao gồm các lời gọi vào một TSF thực hiện bởi các thực thể bên ngoài và phản hồi với các lời gọi này. Các lời gọi thực hiện bởi một TSF không được xem xét rõ ràng trong đánh giá các thành phần, sẽ được mô tả bởi thông tin tin cậy đưa ra nhằm thỏa mãn lớp "Sự tin cậy của thành phần phụ thuộc" (ACO_REL).

16.3.4 ACO_REL.1 Thông tin tin cậy cơ bản

Các mối phụ thuộc: không có sự phụ thuộc nào.

16.3.4.1 Phần tử hành động của nhà phát triển

16.3.4.1.1 ACO_REL.1.1D

Nhà phát triển cần cung cấp thông tin tin cậy của thành phần phụ thuộc.

16.3.4.2 Các phần tử nội dung và trình bày

16.3.4.2.1 ACO_REL.1.1C

Thông tin tin cậy cần mô tả chức năng của thành phần cơ sở như phần cứng, phần sụn và/hoặc phần mềm làm nền tảng cho TSF của thành phần phụ thuộc.

16.3.4.2.2 ACO_REL.1.2C

Thông tin tin cậy cần mô tả tất cả các tương tác thông qua đó TSF của thành phần phụ thuộc yêu cầu dịch vụ từ thành phần cơ sở.

16.3.4.2.3 ACO_REL.1.3C

Thông tin tin cậy cần mô tả cách thức TSF phụ thuộc tự bảo vệ trước sự can thiệp và giả mạo của thành phần cơ sở.

16.3.4.3 Phần tử hành động của đánh giá viên

16.3.4.3.1 ACO_REL.1.1E

Đánh giá viên cần xác nhận rằng thông tin đã cung cấp đáp ứng mọi yêu cầu cho nội dung và hình thức của chứng cứ.

16.3.5 ACO_REL.2 Thông tin tin cậy

Các mối phụ thuộc: không có sự phụ thuộc nào.

16.3.5.1 Phần tử hành động của nhà phát triển

16.3.5.1.1 ACO_REL.2.1D

Nhà phát triển cần cung cấp thông tin tin cậy của thành phần phụ thuộc.

16.3.5.2 Các phần tử nội dung và trình bày

16.3.5.2.1 ACO_REL.2.1C

Thông tin tin cậy cần mô tả chức năng của thành phần cơ sở như phần cứng, phần sụn và/hoặc phần mềm làm nền tảng cho TSF của thành phần phụ thuộc.

16.3.5.2.2 ACO_REL.2.2C

Thông tin tin cậy cần mô tả tất cả các tương tác thông qua đó TSF của thành phần phụ thuộc yêu cầu dịch vụ từ thành phần cơ sở.

16.3.5.2.3 ACO_REL.2.3C

Thông tin tin cậy cần mô tả từng tương tác về giao diện sử dụng và trả lại giá trị từ những giao diện đó.

16.3.5.2.4 ACO_REL.2.4C

Thông tin tin cậy cần mô tả cách thức TSF phụ thuộc tự bảo vệ trước sự can thiệp và giả mạo của thành phần cơ sở.

16.3.5.3 Phần tử hành động của đánh giá viên

16.3.5.3.1 ACO_REL.2.1E

Đánh giá viên cần xác nhận rằng thông tin đã cung cấp đáp ứng mọi yêu cầu cho nội dung và hình thức của chứng cứ.

16.4 Kiểm thử TOE tổng hợp (ACO_CTT)

16.4.1 Mục tiêu

Họ này đòi hỏi thực hiện kiểm thử TOE tổng hợp và kiểm thử thành phần cơ sở, khi được sử dụng trong TOE tổng hợp.

16.4.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở mức chặt chẽ tăng dần của kiểm thử giao diện và mức chặt chẽ tăng dần của phân tích tính đầy đủ của các kiểm thử nhằm thể hiện rằng TSF hoạt động tương ứng với thông tin tin cậy và các SFRs của TOE tổng hợp.

16.4.3 Chú thích ứng dụng

Có hai khía cạnh khác biệt của kiểm kiểm thử liên quan tới họ này:

a) Kiểm thử các giao diện giữa thành phần cơ sở và thành phần phụ thuộc, mà thành phần phụ thuộc dựa vào đó để thực thi chức năng an toàn, nhằm thể hiện tính tương thích của chúng

b) Kiểm thử TOE tổng hợp để thể hiện rằng TOE ứng xử tương ứng với các SFRs của TOE tổng hợp.

Nếu các cấu hình kiểm thử dùng trong đánh giá thành phần phụ thuộc bao gồm việc sử dụng thành phần cơ sở làm "một nền tảng" và việc phân tích kiểm thử đủ để thể hiện rằng TSF tuân thủ với SFRs, nhà phát triển sẽ không cần thực hiện thêm kiểm thử nào nữa cho chức năng của TOE tổng hợp. Tuy nhiên, nếu thành phần cơ sở đã không được sử dụng trong kiểm thử thành phần phụ thuộc, hay cấu hình của một trong hai thành phần thay đổi, khi đó nhà phát triển cần thực hiện kiểm thử cho TOE tổng hợp. Điều đó có thể dẫn đến hình thức nhà phát triển lặp lại các kiểm thử cho thành phần phụ thuộc nhằm đưa ra bằng chứng phù hợp về việc TOE tổng hợp tuân thủ với các SFRs.

Nhà phát triển cần đưa ra chứng cứ về kiểm thử các giao diện thành phần cơ sở đã dùng khi tổng hợp. Hoạt động của TSFIs của thành phần cơ sở có thể đã được kiểm thử trong một phần của lớp ATE: "Các hoạt động kiểm thử" trong đánh giá thành phần cơ sở. Vì vậy, nếu các giao diện thích hợp đã được đưa vào mẫu kiểm thử trong đánh giá thành phần cơ sở và trong lớp "Sở cứ tổng hợp (ACO_COR) đã xác định rằng thành phần cơ sở đang hoạt động tuân theo cấu hình thành phần cơ sở đã đánh giá, với việc mọi chức năng an toàn đòi hỏi bởi thành phần cơ sở đã có trong TSF, thì hành động của đánh giá viên ACO_CTT.1.1E có thể thỏa mãn thông qua việc tái sử dụng thành phần cơ sở ATE: Quyết định kiểm thử.

Nếu không phải như vậy thì các giao diện thành phần cơ sở đã dùng tương ứng cho tổng hợp với sự ảnh hưởng bởi mọi biến đổi về cấu hình đánh giá và mọi chức năng an toàn bổ sung sẽ được kiểm thử nhằm đảm bảo chúng thể hiện hoạt động như mong đợi. Hoạt động mong đợi được kiểm thử là hoạt động đã được mô tả trong thông tin tin cậy (bằng chứng về Sự tin cậy của thành phần phụ thuộc (ACO_REL)).

16.4.4 ACO_CTT.1 Kiểm thử giao diện

Phụ thuộc: ACO_REL.1 Thông tin tin cậy cơ bản
ACO_DEV.1 Mô tả chức năng

16.4.4.1 Mục tiêu

Mục tiêu của thành phần này là nhằm đảm bảo rằng mỗi giao diện của thành phần cơ sở, mà thành phần phụ thuộc dựa vào đó, được kiểm thử.

16.4.4.2 Phần tử hành động của nhà phát triển

16.4.4.2.1 ACO_CTT.1.1D

Nhà phát triển cần đưa ra tài liệu kiểm thử TOE tổng hợp.

16.4.4.2.2 ACO_CTT.1.2D

Nhà phát triển cần đưa ra tài liệu kiểm thử giao diện thành phần cơ sở.

16.4.4.2.3 ACO_CTT.1.3D

Nhà phát triển cần đưa ra TOE tổng hợp để kiểm thử.

16.4.4.2.4 ACO_CTT.1.4D

Nhà phát triển cần đưa ra một tập tài nguyên tương đương với tập dùng trong kiểm thử chức năng thành phần cơ sở của nhà phát triển.

16.4.4.3 Các phần tử nội dung và trình bày

16.4.4.3.1 ACO_CTT.1.1C

Tài liệu kiểm thử cho TOE tổng hợp và giao diện thành phần cơ sở cần bao gồm kế hoạch kiểm thử, kết quả kiểm thử dự kiến kết quả kiểm thử thực tế.

16.4.4.3.2 ACO_CTT.1.2C

Tài liệu kiểm thử có được từ việc nhà phát triển thực hiện kiểm thử TOE tổng hợp cần chứng tỏ rằng TSF tuân thủ theo quy định.

16.4.4.3.3 ACO_CTT.1.3C

Tài liệu kiểm thử có được từ việc nhà phát triển thực hiện kiểm thử thành phần cơ sở cần chứng tỏ rằng giao diện thành phần cơ sở mà thành phần cơ sở dựa vào tuân thủ theo quy định.

16.4.4.3.4 ACO_CTT.1.4C

Thành phần cơ sở cần thích hợp cho kiểm thử.

16.4.4.4 Phần tử hành động của đánh giá viên

16.4.4.4.1 ACO_CTT.1.1E

Đánh giá viên cần xác nhận rằng thông tin đã cung cấp đáp ứng mọi yêu cầu cho nội dung và hình thức của chứng cứ.

16.4.4.4.2 ACO_CTT.1.2E

Đánh giá viên cần thực hiện một kiểm thử mẫu trong tài liệu kiểm thử để kiểm nghiệm các kết quả kiểm thử của nhà phát triển.

16.4.4.4.3 ACO_CTT.1.3E

Đánh giá viên cần kiểm thử một tập con các giao diện TSF của TOE tổng hợp để khẳng định rằng TSF tổng hợp hoạt động theo quy định.

16.4.5 ACO_CTT.2 Kiểm thử giao diện chặt chẽ

Phụ thuộc: ACO_REL.2 Thông tin tin cậy
ACO_DEV.2 Chứng cứ cơ bản của thiết kế

16.4.5.1 Mục tiêu

Mục tiêu của thành phần này là để đảm bảo rằng mỗi giao diện của thành phần cơ sở, mà thành phần phụ thuộc dựa vào nó, được kiểm thử.

16.4.5.2 Phần tử hành động của nhà phát triển

16.4.5.2.1 ACO_CTT.2.1D

Nhà phát triển cần đưa ra tài liệu kiểm thử TOE tổng hợp.

16.4.5.2.2 ACO_CTT.2.2D

Nhà phát triển cần đưa ra tài liệu kiểm thử giao diện thành phần cơ sở.

16.4.5.2.3 ACO_CTT.2.3D

Nhà phát triển cần đưa ra TOE tổng hợp để kiểm thử.

16.4.5.2.4 ACO_CTT.2.4D

Nhà phát triển cần đưa ra một tập tài nguyên tương đương với tập dùng trong kiểm thử chức năng thành phần cơ sở của nhà phát triển.

16.4.5.3 Các phần tử nội dung và trình bày

16.4.5.3.1 ACO_CTT.2.1C

Tài liệu kiểm thử cho TOE tổng hợp và giao diện thành phần cơ sở cần bao gồm kế hoạch kiểm thử, kết quả kiểm thử dự kiến kết quả kiểm thử thực tế.

16.4.5.3.2 ACO_CTT.2.2C

Tài liệu kiểm thử có được từ việc nhà phát triển thực hiện kiểm thử TOE tổng hợp cần chứng tỏ rằng TSF tuân thủ theo quy định **và đầy đủ**.

16.4.5.3.3 ACO_CTT.2.3C

Tài liệu kiểm thử có được từ việc nhà phát triển thực hiện kiểm thử thành phần cơ sở cần chứng tỏ rằng giao diện thành phần cơ sở mà thành phần cơ sở dựa vào tuân thủ theo quy định **và đầy đủ**.

16.4.5.3.4 ACO_CTT.2.4C

Thành phần cơ sở cần thích hợp cho kiểm thử.

16.4.5.4 Phần tử hành động của đánh giá viên

16.4.5.4.1 ACO_CTT.2.1E

Đánh giá viên cần xác nhận rằng thông tin đã cung cấp đáp ứng mọi yêu cầu cho nội dung và hình thức của chứng cứ.

16.4.5.4.2 ACO_CTT.2.2E

Đánh giá viên cần thực hiện một kiểm thử mẫu trong tài liệu kiểm thử để kiểm nghiệm các kết quả kiểm thử của nhà phát triển.

16.4.5.4.3 ACO_CTT.2.3E

Đánh giá viên cần kiểm thử một tập con các giao diện TSF của TOE tổng hợp để khẳng định rằng TSF tổng hợp hoạt động theo quy định.

16.5 Phân tích điểm yếu tổng hợp (ACO_VUL)

16.5.1 Mục tiêu

Họ này dùng cho phân tích thông tin điểm yếu sẵn có thông báo công khai và các điểm yếu có thể sẽ nảy sinh khi tổng hợp.

16.5.2 Phân mức thành phần

Các thành phần trong họ này được phân mức trên cơ sở khảo sát kỹ lưỡng với mức tăng dần thông tin điểm yếu đã thông báo công khai và phân tích điểm yếu một cách độc lập.

16.5.3 Chú thích ứng dụng

Nhà phát triển sẽ cung cấp chi tiết của mọi điểm yếu còn lại ghi nhận trong đánh giá các thành phần. Điều này có thể đạt được từ các nhà phát triển thành phần hoặc từ các báo cáo đánh giá thành phần. Những thông tin này sẽ được sử dụng làm đầu vào cho phân tích điểm yếu của TOE tổng hợp trong môi trường vận hành.

Môi trường vận hành của TOE tổng hợp được kiểm tra nhằm đảm bảo rằng các giả định và mục tiêu cho môi trường vận hành thành phần (quy định cho từng ST thành phần) được thoả mãn trong TOE tổng hợp. Một phân tich ban đầu về tính nhất quán của các giả định và mục tiêu giữa các thành phần và các STs của TOE tổng hợp sẽ được thực hiện trong khi tiến hành các hoạt động ASE cho TOE tổng hợp. Tuy nhiên, việc phân tích này được nhắc lại với những hiểu biết thu được trong các hoạt động ACO_REL, ACO_DEV và ACO_COR nhằm đảm bảo rằng, ví dụ, các giả định về thành phần phụ thuộc đã được đề cập đến trong môi trường trong ST của thành phần phụ thuộc sẽ không được nhắc lại trong kết quả tổng hợp (nghĩa là thành phần cơ sở đề cập một cách tương xứng các giả định về ST của thành phần phụ thuộc trong TOE tổng hợp).

Đánh giá viên sẽ tìm kiếm các vấn đề trong mỗi thành phần, xác định các điểm yếu tiềm ẩn đã thông báo trên phạm vi công cộng sau khi hoàn tất đánh giá các thành phần. Mọi điểm yếu tiềm ẩn sẽ được kiểm thử.

Nếu thành phần cơ sở đã dùng trong TOE tổng hợp trở thành chủ đề của các hoạt động duy trì bảo đảm kể từ khi có chứng nhận, đánh giá viên sẽ xem xét trong các hoạt động phân tích điểm yếu của TOE tổng hợp những thay đổi đã thực hiện trong thành phần cơ sở.

16.5.4 ACO_VUL.1 Soát xét điểm yếu tổng hợp

Phụ thuộc: ACO_DEV.1 Mô tả chức năng

16.5.4.1 Phần tử hành động của nhà phát triển

16.5.4.1.1 ACO_VUL.1.1D

Nhà phát triển cần đưa ra TOE tổng hợp để kiểm thử.

16.5.4.2 Các phần tử nội dung và trình bày

16.5.4.2.1 ACO_VUL.1.1C

TOE tổng hợp cần thích hợp cho kiểm thử.

16.5.4.3 Phần tử hành động của đánh giá viên

16.5.4.3.1 ACO_VUL.1.1E

Đánh giá viên cần xác nhận rằng thông tin đã cung cấp đáp ứng mọi yêu cầu cho nội dung và hình thức của chứng cứ.

16.5.4.3.2 ACO_VUL.1.2E

Đánh giá viên cần thực hiện phân tích nhằm xác định mọi điểm yếu vốn có xác định cho thành phần cơ sở và thành phần phụ thuộc không bị khai thác trong TOE tổng hợp và môi trường vận hành của nó.

16.5.4.3.3 ACO_VUL.1.3E

Đánh giá viên cần thực hiện tìm kiếm các nguồn thông tin công cộng để xác định các điểm yếu có thể phát sinh từ việc dùng các thành phần cơ sở và thành phần phụ thuộc trong môi trường vận hành TOE tổng hợp.

16.5.4.3.4 ACO_VUL.1.4E

Đánh giá viên cần tiến hành kiểm thử xâm nhập, dựa trên các điểm yếu đã xác định, để chứng minh rằng TOE tổng hợp được bảo vệ trước các tấn công bởi kẻ tấn công có tiềm năng tấn công cơ bản.

16.5.5 ACO_VUL.2 Phân tích điểm yếu tổng hợp

Phụ thuộc: ACO_DEV.2 Chứng cứ cơ bản của thiết kế

16.5.5.1 Phần tử hành động của nhà phát triển

16.5.5.1.1 ACO_VUL.2.1D

Nhà phát triển cần đưa ra TOE tổng hợp để kiểm thử.

16.5.5.2 Các phần tử nội dung và trình bày

16.5.5.2.1 ACO_VUL.2.1C

TOE tổng hợp cần thích hợp cho kiểm thử.

16.5.5.3 Phần tử hành động của đánh giá viên

16.5.5.3.1 ACO_VUL.2.1E

Đánh giá viên cần xác nhận rằng thông tin đã cung cấp đáp ứng mọi yêu cầu cho nội dung và hình thức của chứng cứ.

16.5.5.3.2 ACO_VUL.2.2E

Đánh giá viên cần thực hiện phân tích nhằm xác định mọi điểm yếu vốn có xác định cho thành phần cơ sở và thành phần phụ thuộc không bị khai thác trong TOE tổng hợp và môi trường vận hành của nó.

16.5.5.3.3 ACO_VUL.2.3E

Đánh giá viên cần thực hiện tìm kiếm các nguồn thông tin công cộng để xác định các điểm yếu có thể phát sinh từ việc dùng các thành phần cơ sở và thành phần phụ thuộc trong môi trường vận hành TOE tổng hợp.

16.5.5.3.4 ACO_VUL.2.4E

Đánh giá viên cần thực hiện phân tích điểm yếu độc lập cho TOE tổng hợp thông qua sử dụng tài liệu hướng dẫn, thông tin tin cậy và sở cứ tổng hợp nhằm xác định các điểm yếu tiềm ẩn trong TOE tổng hợp.

16.5.5.3.5 ACO_VUL.2.5E

Đánh giá viên cần tiến hành kiểm thử xâm nhập, dựa trên các điểm yếu đã xác định, để chứng minh rằng TOE tổng hợp được bảo vệ trước các tấn công bởi kẻ tấn công có tiềm năng tấn công cơ bản.

16.5.6 ACO_VUL.3 Phân tích điểm yếu tổng hợp cơ bản - nâng cao

Phụ thuộc: ACO_DEV.3 Chứng cứ chi tiết về thiết kế

16.5.6.1 Phần tử hành động của nhà phát triển

16.5.6.1.1 ACO_VUL.3.1D

Nhà phát triển cần đưa ra TOE tổng hợp để kiểm thử.

16.5.6.2 Các phần tử nội dung và trình bày

16.5.6.2.1 ACO_VUL.3.1C

TOE tổng hợp cần thích hợp cho kiểm thử.

16.5.6.3 Phần tử hành động của đánh giá viên

16.5.6.3.1 ACO_VUL.3.1E

Đánh giá viên cần xác nhận rằng thông tin đã cung cấp đáp ứng mọi yêu cầu cho nội dung và hình thức của chứng cứ.

16.5.6.3.2 ACO_VUL.3.2E

Đánh giá viên cần thực hiện phân tích nhằm xác định mọi điểm yếu vốn có xác định cho thành phần cơ sở và thành phần phụ thuộc không bị khai thác trong TOE tổng hợp và môi trường vận hành của nó.

16.5.6.3.3 ACO_VUL.3.3E

Đánh giá viên cần thực hiện tìm kiếm các nguồn thông tin công cộng để xác định các điểm yếu có thể phát sinh từ việc dùng các thành phần cơ sở và thành phần phụ thuộc trong môi trường vận hành TOE tổng hợp.

16.5.6.3.4 ACO_VUL.3.4E

Đánh giá viên cần thực hiện phân tích điểm yếu độc lập cho TOE tổng hợp thông qua sử dụng tài liệu hướng dẫn, thông tin tin cậy và sở cứ tổng hợp nhằm xác định các điểm yếu tiềm ẩn trong TOE tổng hợp.

16.5.6.3.5ACO_VUL.3.5E

Đánh giá viên cần tiến hành kiểm thử xâm nhập, dựa trên các điểm yếu đã xác định, để chứng minh rằng TOE tổng hợp được bảo vệ trước các tấn công bởi kẻ tấn công có tiềm năng tấn công cơ bản.

Phụ lục A

(Tham khảo)

Lớp phát triển (ADV)

Phụ lục này có chứa tài liệu phụ trợ để tiếp tục giải thích và cung cấp các ví dụ bổ sung cho các chủ đề đưa ra trong các họ của lớp ADV: Lớp Phát triển.

A.1 ADV_ARC: Bổ sung các tài liệu trên kiến trúc an toàn

Một kiến trúc an toàn là một bộ các thuộc tính mà TSF trình bày; những thuộc tính này bao gồm tự bảo vệ, tách miền, và non-bypassability. Có những thuộc tính cung cấp cơ sở tin cậy để TSF cung cấp những dịch vụ an toàn của nó. Phụ lục này cung cấp tài liệu bổ sung trên các thuộc tính đó, cũng như những thảo luận về nội dung của một mô tả kiến trúc an toàn.

Ngoài ra mục này, trước hết sẽ giải thích những thuộc tính đó, sau đó thảo luận về những loại thông tin cần thiết để mô tả cách TSF trình bày những thuộc tính đó.

A.1.1 Các thuộc tính trong kiến trúc an toàn

Tự bảo vệ đề cập đến khả năng TSF bảo vệ cho chính nó bằng thao tác từ các thực thể bên ngoài mà vẫn có thể dẫn đến những thay đổi trong TSF. Nếu thiếu những thuộc tính này, các TSF có thể bị vô hiệu hóa khi thực hiện các dịch vụ an toàn của nó.

Đôi khi có trường hợp mà một TOE sử dụng các dịch vụ hoặc nguồn tài nguyên cung cấp bởi các thực thể CNTT khác để thực hiện chức năng của nó (ví dụ như một ứng dụng dựa trên hệ điều hành cơ bản của nó). Trong những trường hợp này, các TSF không tự bảo vệ mình hoàn toàn, bởi vì nó phụ thuộc vào các thực thể IT khác để bảo vệ các dịch vụ nó sử dụng.

Tách miền là một thuộc tính theo đó TSF tạo ra các miền an toàn riêng cho từng thực thể hành động không tin cậy để hoạt động trên tài nguyên của nó, và sau đó giữ những miền đó được tách biệt khỏi những thực thể còn lại để không thực thể nào có thể chạy trên miền của bất kỳ thực thể khác. Ví dụ, một TOE hệ điều hành sẽ cấp một tên miền (không gian địa chỉ, biến môi trường trên một tiến trình) cho từng tiến trình liên kết với các thực thể không tin cậy.

Đối với một số TOE tên miền không tồn tại vì tất cả các hành động của các thực thể không tin cậy được đưa ra bởi TSF. Một bức tường lửa lọc gói là một ví dụ của TOE như vậy, nơi không có những tên miền của thực thể không tin cậy; chỉ có những cấu trúc dữ liệu chỉ được duy trì bởi các TSF. Trong trường hợp mà ở đó TOE không cung cấp tên miền cho những thực thể không tin cậy, họ này yêu cầu những tên miền đó phải được cô lập khỏi những miền khác, như vậy những thực thể không tin cậy trong một miền bị ngăn chặn việc giả mạo từ các miền khác của thực thể không tin cậy.

Non-bypassability là một thuộc tính mà các chức năng an toàn của TSF (đặc tả bởi SFR) luôn được yêu cầu và không thể bị phá vỡ, thích hợp cho cơ chế cụ thể. Ví dụ, nếu việc điều khiển truy cập vào các tệp được quy định như một khả năng của TSF qua một SFR, thì không cần có giao diện mà thông qua đó các tập tin có thể được truy cập mà không cần viện dẫn cơ chế điều khiển truy cập của TSF.

Như là trường hợp tự bảo vệ, chính bản chất của một số TOE có thể phụ thuộc vào môi trường của chúng để đóng vai trò trong non-bypassability của TSF. Ví dụ, một TOE ứng dụng an toàn yêu cầu rằng nó được gọi bởi hệ điều hành cơ bản. Tương tự như vậy, tường lửa phụ thuộc vào thực tế là không có kết nối trực tiếp giữa các mạng nội bộ và bên ngoài và tất cả lưu lượng giữa chúng phải đi qua tường lửa.

A.1.2 Mô tả kiến trúc an toàn

Mô tả kiến trúc an toàn giải thích cách các thuộc tính mô tả ở trên được trình bày bởi các TSF. Nó mô tả các miền được định nghĩa thế nào và TSF giữ chúng riêng biệt như thế nào. Nó mô tả cái gì ngăn chặn các tiến trình không tin cậy khỏi việc nhận TSF và sửa đổi nó. Nó mô tả cái gì đảm bảo rằng tất cả các tài nguyên thuộc quyền kiểm soát của TSF được bảo vệ đầy đủ và tất cả các hành động liên quan đến SFR được dàn xếp bởi TSF. Nó giải thích vai trò bất kỳ mà môi trường đó thực hiện trong bất kỳ những vai trò đó (ví dụ: giả sử nó được gọi ra một cách chính xác bởi môi trường cơ sở của nó, làm thế nào các chức năng an toàn của nó được gọi ra?).

Mô tả kiến trúc an toàn trình bày các thuộc tính tự bảo vệ, tách miền, và non-bypassability của TSF trong một giới hạn mô tả phân tích. Mức độ mô tả này là tương xứng với sự mô tả TSF yêu cầu bởi những yêu cầu ADV_FSP, ADV_TDS và ADV_IMP đang được tuyên bố. Ví dụ, nếu ADV_FSP chỉ là mô tả TSF sẵn có, thì ADV_FSP sẽ thật khó để đưa ra bất kỳ thiết kế kiến trúc có ý nghĩa bởi vì không chi tiết nào của bất kỳ hoạt động bên trong TSF sẽ được sẵn sàng.

Tuy nhiên, nếu thiết kế TOE cũng có sẵn, ngay cả ở mức cơ bản nhất (ADV_TDS.1), thì sẽ có các thông tin liên quan đến các hệ thống con tạo nên TSF, và sẽ có một mô tả về cách chúng làm việc thế nào để thực thi những thuộc tính tự bảo vệ, tách miền, và none- bypassability. Ví dụ, có thể tất cả các tương tác người dùng với TOE là hạn chế thông qua một tiến trình mà có các hành động đại diện cho người dùng, chấp nhận tất cả các thuộc tính an toàn của người dùng; các thiết kế kiến trúc sẽ mô tả một tiến trình diễn ra thế nào, cách xử lý của tiến trình bị hạn chế bởi các TSF thế nào (để nó có thể không bị ngắt bởi TSF), tất cả các hành động của tiến trình đó được giàn xếp bởi TSF thế nào (do đó giải thích tại sao các TSF không thể bỏ qua), v.v...

Nếu việc thiết kế một TOE chi tiết hơn (ví dụ như ở cấp độ mô-đun), hoặc các đại diện thực thi cũng sẵn sàng, thì sau đó mô tả của thiết kế kiến trúc tương ứng chi tiết hơn, giải thích được tiến trình người dùng truyền thông với tiến trình TSF thế nào, cách các yêu cầu khác nhau được xử lý bởi các TSF thế nào, những tham số gì được thông qua, những chương trình bảo vệ nào (chống tràn bộ đệm, kiểm tra các thông số giới hạn, thời gian kiểm tra/thời gian kiểm tra sử dụng, v.v...) được đưa ra. Tương tự, một TOE, mà ST của TOE này yêu cầu có thành phần ADV_IMP, sẽ đi vào chi tiết thực thi cụ thể.

Các giải trình cung cấp trong mô tả kiến trúc an toàn dự kiến sẽ được chi tiết đầy đủ, có thể kiểm thử tính chính xác của chúng. Chẳng hạn, một khẳng định đơn giản (ví dụ: "TSF duy trì sự riêng rẽ các miền") không cung cấp thông tin hữu ích để thuyết phục người đọc rằng TSF quả thực tạo và phân tách miền riêng biệt.

A.1.2.1 Tách miền

Trong trường hợp TOE trình bày sự phân tách miền một cách hoàn toàn riêng mình nó, sẽ có một mô tả đơn giản về cách mà điều này đạt được. Mô tả kiến trúc an toàn có thể giải thích các loại khác nhau của các miền được xác định bởi TSF, cách chúng được định nghĩa (tức là những tài nguyên nào được phân bổ cho từng miền), và cách các miền được giữ phân tách ra để các thực thể hành động trong một miền không thể làm xáo trộn các tài nguyên trong miền khác.

Đối với trường hợp TOE phụ thuộc vào các thực thể CNTT khác để thực hiện một vai trò trong miền tách, thì việc chia sẻ về vai trò đó phải được làm rõ. Ví dụ, một TOE mà chỉ duy nhất phần mềm ứng dụng dựa vào hệ điều hành cơ sở để khởi tạo chính xác các miền mà TOE đó định nghĩa; nếu TOE đó định nghĩa không gian xử lý riêng biệt, không gian bộ nhớ, v.v.. đối với mỗi miền, thì nó phụ thuộc vào hệ điều hành cơ sở để hoạt động một cách chính xác và benignly (ví dụ như cho phép quá trình thực hiện chỉ trong không gian thực hiện được yêu cầu bởi phần mềm TOE).

Ví dụ, cơ chế thực hiện tách miền (vi dụ như quản lý bộ nhớ, bảo vệ chế độ quy trình cung cấp bởi phần cứng, v.v...) sẽ được xác định và mô tả. Hoặc, TSF có thể thực thi các cấu trúc bảo vệ phần mềm hoặc các quy ước mã hóa góp phần thực thi việc tách của các miền phần mềm, có thể bằng cách phân định không gian địa chỉ người sử dụng từ không gian địa chỉ hệ thống.

Các phân tích tính điểm yếu và hoạt động kiểm thử (xem AVA_VAN) có khả năng sẽ bao gồm các nỗ lực để làm hỏng sự phân tách miền TSF được mô tả, thông qua việc sử dụng các giám sát hoặc tấn công trực tiếp các TSF.

A.1.2.2 TSF Tự bảo vệ

Trong trường hợp TOE trình bày tự bảo vệ hoàn toàn tự nó, sẽ có một mô tả đơn giản về cách tự bảo vệ này đạt được. Cơ chế cung cấp cho việc tách miền để xác định một miền TSF được bảo vệ khỏi những miền khác (người sử dụng) sẽ được xác định và mô tả.

Đối với trường hợp TOE phụ thuộc vào các thực thể CNTT khác để thực hiện vai trò trong việc bảo vệ chính nó, thì việc chia sẻ về vai trò đó phải được làm rõ. Ví dụ, một TOE mà chỉ duy nhất phần mềm ứng dụng dựa vào hệ điều hành cơ sở để hoạt động chính xác; các ứng dụng không thể tự bảo vệ mình chống lại một hệ điều hành độc hại mà phá hoại nó (ví dụ, bằng cách ghi đè mã thực thi của nó hoặc TSF dữ liệu).

Mô tả kiến trúc bảo mật cũng bao trùm việc đầu vào người dùng được xử lý bởi các TSF như thế nào theo cách mà các TSF không để chính bản thân chủ thể bị ngắt bởi đầu vào người dùng đó. Ví dụ, TSF có thể thực thi khái niệm đặc quyền và tự bảo vệ mình bằng cách sử dụng các routines chế độ có đặc quyền xử lý dữ liệu người dùng. Các TSF có thể tận dụng các cơ chế phân chia bộ xử lý cơ sở (ví dụ như các mức độ hoặc vòng đặc quyền) để tách mã và dữ liệu TSF từ mã và dữ liệu người dùng. Các TSF có thể thực thi các cấu trúc bảo vệ phần mềm hoặc các quy ước mã hóa đó góp phần thực thi việc tách của phần mềm, có thể bằng cách phân định không gian địa chỉ người sử dụng từ không gian địa chỉ hệ thống.

Đối với các TOE khởi động trong một chế độ chức năng thấp (ví dụ, một chế độ một người dùng đơn chỉ có thể dùng đối với người cài đặt hoặc các quản trị viên) và sau đó chuyển tiếp sáng cấu hình an toàn đã được đánh giá (một chế độ mà nhờ đó những người dùng không tin cậy có thể đăng nhập và sử dụng dịch vụ và tài nguyên của TOE), mô tả kiến trúc an toàn cũng bao gồm phần giải thích về cách các TSF được bảo vệ chống lại các mã khởi động mà không chạy trong cấu hình đã được đánh giá. Đối với các TOE như vậy, sự mô tả kiến trúc an toàn sẽ giải thích cái gì ngăn cản các dịch vụ mà nên sẵn có trong suốt thời gian khởi động (ví dụ như truy cập trực tiếp đến các nguồn tài nguyên) khỏi bị truy cập trong cấu hình đánh giá. Nó cũng sẽ giải thích cái gì ngăn cản mã khởi động chạy khi các TOE là đang trong cấu hình đã được đánh giá đó.

Cũng phải có một giải thích về cách mã khởi động tin cậy sẽ duy trì tính toàn vẹn của TSF (và của quá trình khởi động của nó), như vậy mà quá trình khởi động có thể phát hiện bất kỳ sửa đổi nào cho kết quả trong TSF là giả mạo để tin rằng đó là một trạng thái an toàn ban đầu.

Các phân tích tính điểm yếu và hoạt động kiểm thử (xem AVA_VAN) có khả năng sẽ bao gồm các nỗ lực để làm hỏng TSF tự bảo vệ được mô tả, thông qua việc sử dụng các can thiệp, tấn công trực tiếp, hoặc giám sát của TSF.

A.1.2.3 TSF Không bỏ qua

Thuộc tính của không bỏ qua liên quan với các giao diện cho phép bỏ qua các cơ chế thực thi bắt buộc. Trong hầu hết các trường hợp điều này là hệ quả của việc thực thi, nơi mà nếu một người lập trình đang viết giao diện để truy cập hoặc thao tác một đối tượng, thì đó là trách nhiệm của người lập trình sử dụng giao diện mà giao diện đó là một phần của cơ chế thực thi SFR cho đối tượng và không

để cố gắng phá vỡ những giao diện đó. Đối với các mô tả gắn liền với non-bypassabilit có hai phạm vi khái quát phải được bao trùm.

Đầu tiên bao gồm các giao diện cho việc thi hành-SFR. Các thuộc tính cho các giao diện này là để chúng không chứa các hoạt động hoặc chế độ cho phép chúng được sử dụng để bỏ qua các TSF. Có khả năng là các bằng chứng cho ADV_FSP và ADV_TDS có thể được sử dụng trong phần lớn để quyết định. Bởi vì non-bypassability là mối quan tâm, nếu chỉ các hoạt động nhất định sẵn có thông qua các TSFI được tài liệu hóa (vì chúng là SFR- thi hành) còn những hoạt động khác thì không, thì nhà phát triển nên cân nhắc liệu thông tin bổ sung (trình bày trong ADV_FSP và ADV_TDS) có cần thiết để thực hiện một quyết định rằng hoạt động của TSFI SFR-hỗ trợ và SFR-không can thiệp không đủ điều kiện cho một thực thể không tin cậy có khả năng bỏ qua các chính sách được thi hành. Nếu như các thông tin là cần thiết, nó sẽ có trong các mô tả kiến trúc an ninh.

Phạm vi thứ hai của non-bypassability quan tâm đến những giao diện mà tương tác của nó không liên quan đến SFR-thực thi. Tùy thuộc vào thành phần ADV_FSP và ADV_TDS được tuyên bố, một số thông tin về các giao diện này có thể hoặc không thể tồn tại trong đặc tả chức năng và tài liệu thiết kế TOE. Thông tin trình bày cho các giao diện đó (hoặc nhóm các giao diện) nên đầy đủ để người đọc có thể đưa ra một quyết định (ở mức độ chi tiết tương xứng với phần còn lại của bằng chứng được cung cấp trong ADV: Lớp phát triển) mà các cơ chế thi hành không thể được bỏ qua.

Thuộc tính mà các chức năng an toàn không thể bỏ qua áp dụng như nhau cho tất cả các chức năng an toàn. Đó là, mô tả thiết kế nên bao trùm các đối tượng được bảo vệ dưới các SFR (ví dụ như các thành phần * FDP_) và chức năng (ví dụ, kiểm toán) được cung cấp bởi TSF. Mô tả cũng nên xác định giao diện có liên quan đến chức năng an toàn; điều này có thể tạo việc sử dụng các thông tin trong các đặc tả chức năng. Mô tả này cũng nên mô tả bất kỳ cấu trúc thiết kế nào, chẳng hạn như các nhà quản lý đối tượng, và phương pháp sử dụng của họ. Ví dụ, nếu các thường trình (routines) sử dụng một macro tiêu chuẩn để tạo ra một bản ghi kiểm toán, quy ước này là một phần của thiết kế mà nó góp phần vào việc non-bypassability của cơ chế kiểm toán. Điều quan trọng cần lưu ý là non-bypassability trong bối cảnh này không phải là một cố gắng để trả lời câu hỏi "có thể là một phần của việc thực hiện TSF, nếu là các mã độc, thì bỏ qua các chức năng an toàn", mà nên đưa ra cách làm thế nào để việc thực thi không bỏ qua chức năng an toàn.

Các phân tích tính điểm yếu và hoạt động kiểm thử (xem AVA_VAN) có thể sẽ bao gồm các nỗ lực để thất bại non-bypassability đã được mô tả, nhờ việc phá hỏng các TSF.

A.2 ADV_FSP: Bổ sung các tài liệu trên các TSFI

Mục đích cụ thể TSFIs là cung cấp những thông tin cần thiết để tiến hành kiểm thử; thiếu những thông tin về phương tiện có thể tương tác với các TSF, thì TSFI đó không thể kiểm thử cách xử lý củacác TSF.

Có hai phần để xác định TSFIs: xác định chúng và mô tả chúng. Vì sự đa dạng của các TOE, và của TSF khác nhau trong đó, không có bộ tiêu chuẩn giao diện tạo thành "TSFI". Phụ lục này cung cấp hướng dẫn về các yếu tố xác định các giao diện nào là TSFIs.

A.2.1 Xác định TSFI

Để xác định các giao diện cho TSF, các phần của TOE tạo nên TSF trước tiên phải được xác định. Nhận dạng này thực sự là một phần của các phân tích thiết kế TOE (ADV_TDS),-nhưng cũng được thực hiện hoàn toàn (thông qua nhận dạng và mô tả của các TSFI) bởi nhà phát triển trong trường hợp thiết kế TOE (ADV_TDS) không nằm trong gói đảm bảo. Trong phân tích này, một phần của TOE phải được coi là trong TSF nếu nó góp phần vào sự đáp ứng của một SFR trong ST (toàn bộ hoặc một phần). Điều này bao gồm, ví dụ, tất cả mọi thứ trong TOE góp phần cho TSF sự khởi động chạy theo

thời gian, chẳng hạn như phần mềm chạy trước khi TSF có khả năng tự bảo vệ mình vì việc thi hành SFR chưa bắt đầu (Ví dụ, trong khi khởi động lên). Cũng bao gồm trong TSF là tất cả các phần của TOE đóng góp vào các nguyên tắc kiến trúc của TSF tự bảo vệ, tách miền, và non-bypassability (xem Kiến trúc an toàn (ADV_ARC)).

Một khi các TSF đã được định nghĩa, các TSFI được xác định. Các TSFI bao gồm tất cả các phương tiện cho người dùng gọi một dịch vụ từ TSF (bằng cách cung cấp dữ liệu được xử lý bởi các TSF) và các phản ứng tương ứng với những yêu cầu dịch vụ đó. Những yêu cầu và hồi đáp dịch vụ là các phương tiện đi qua ranh giới TSF. Trong khi nhiều yêu cầu và hồi đáp dịch vụ trong số này là rõ ràng, còn lại có thể không rõ ràng. Một câu hỏi nên được yêu cầu khi xác định TSFI là: "Làm thế nào một kẻ tấn công tiềm ẩn có thể tương tác với các TSF trong một nỗ lực để phá vỡ các SFR?" Các cuộc thảo luận sau đây minh họa việc áp dụng định nghĩa TSFI trong các ngữ cảnh khác nhau.

A.2.1.1 Giao diện điện

Trong các TOE chẳng hạn như thẻ thông minh, nơi mà kẻ thù không chỉ truy cập vào TOE về logic, mà còn hoàn toàn truy cập vật lý vào TOE, ranh giới TSF là ranh giới vật lý. Do đó, giao diện điện tử phô ra được xem là TSFI bởi vì thao tác của chúng có thể ảnh hưởng đến cách xử lý của TSF. Như vậy, tất cả các giao diện này (các liên hệ điện tử) cần phải được mô tả: các điện áp khác nhau có thể được áp dụng, v.v....

A.2.1.2 Ngăn xếp giao thức mạng

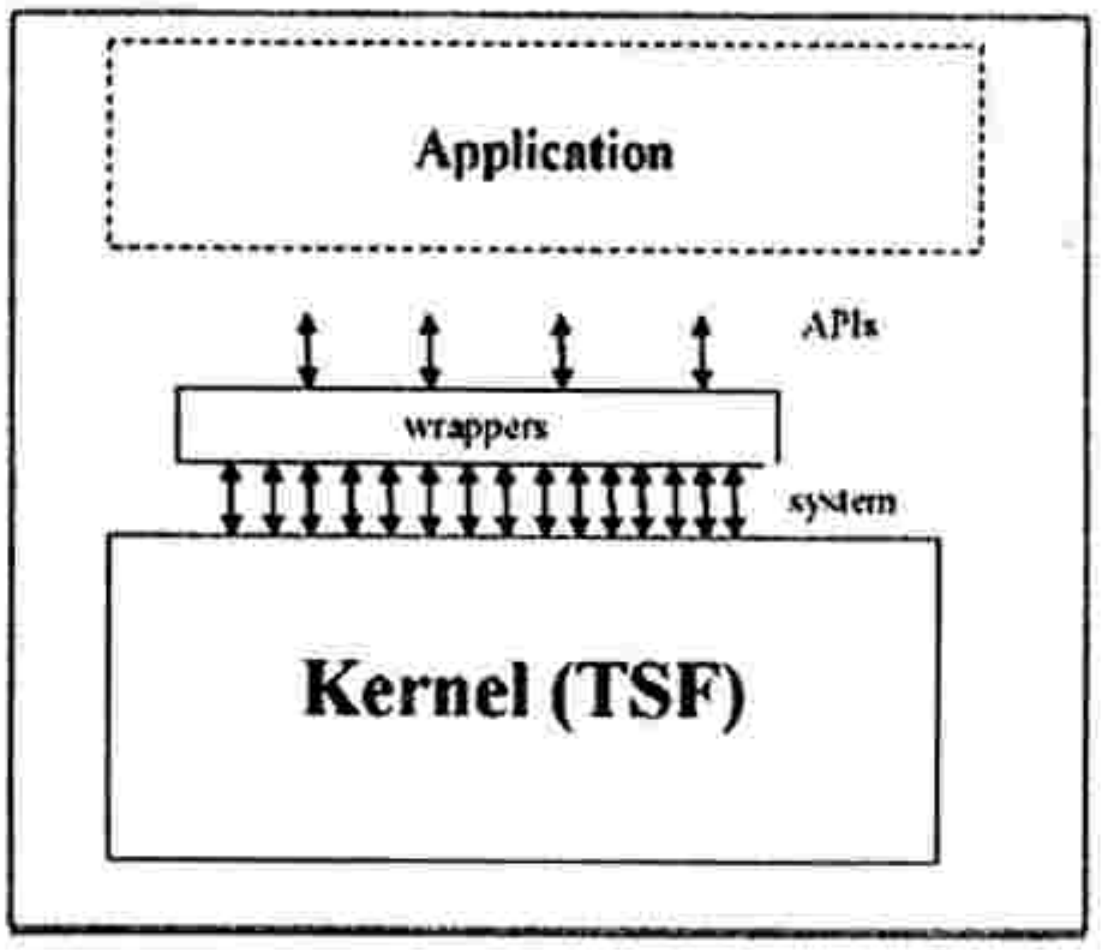
Các TSFIs của một TOE mà thực hiện xử lý giao thức sẽ là những lớp giao thức mà một kẻ tấn công tiềm ẩn có thể truy cập trực tiếp. Điều này không nhất thiết là toàn bộ chồng giao thức.

Ví dụ, nếu các TOE là một số loại của một thiết bị mạng cho phép kẻ tấn công tiềm ẩn làm ảnh hưởng đến các lớp của chồng giao thức (tức là để gửi tín hiệu tùy ý, điện áp bất kỳ, các gói tin bất kỳ, gói dữ liệu bất kỳ, v.v...), sau đó là ranh giới TSF tồn tại ở mỗi lớp của chồng giao thức đó. Do đó, đặc tả chức năng sẽ phải hướng đến giao thức ở mỗi lớp của chồng giao thức đó.

Tuy nhiên, nếu các TOE là một tường lửa bảo vệ mạng nội bộ từ Internet, một kẻ tấn công tiềm ẩn sẽ không có phương tiện thao tác trực tiếp điện áp vào TOE; bất kỳ điện áp cực đại nào cũng sẽ không đơn giản được cho qua thông qua Internet. Đó là, kẻ tấn công sẽ có quyền truy cập chỉ với những giao thức tại lớp Internet hoặc ở trên. Ranh giới TSF tồn tại ở mỗi lớp của chồng giao thức. Vì vậy, đặc tả chức năng sẽ phải nhắm đến chỉ những giao thức ở tại lớp Internet hoặc lớp phía trên: nó sẽ mô tả mỗi lớp truyền thông khác nhau mà tại đó tường lửa được phô ra dưới dạng những thứ tạo nên đầu vào đúng cho cái có thể xuất hiện trên đường truyền, và kết quả của cả hai đầu vào đúng và dị hình. Ví dụ, mô tả về lớp giao thức Internet sẽ mô tả cái tạo ra một gói tin IP đúng và những gì xảy ra khi cả hai dạng gói tin đúng và gói tin dị hình đều được nhận. Tương tự, sự mô tả của lớp TCP sẽ mô tả một kết nối TCP thành công và những gì xảy ra cả khi các kết nối thành công được thiết lập và khi kết nối không thể được thiết lập hoặc bị mất không cố ý. Lợi dụng mục đích của tường lửa là để lọc các lệnh ở cấp ứng dụng (như FTP hoặc telnet), mô tả lớp ứng dụng sẽ mô tả các lệnh ở cấp ứng dụng đó để tường lửa nhận ra và lọc, cũng như kết quả của việc gặp phải lệnh không rõ.

Những mô tả của các lớp này có thể tham khảo ở các tiêu chuẩn truyền thông đã phát hành (telnet, FTP, TCP, v.v...) đang được sử dụng.

A.2.1.3 Trình bao bọc (Wrappers)



Hình A.1 – Bộ wrapper (trình bao bọc)

"Wrappers" biên dịch loạt các tương tác phức tạp thành các dịch vụ phổ biến đơn giản hóa, chẳng hạn như khi Hệ điều hành tạo ra các API để sử dụng bởi các ứng dụng (như trong Hình A.1). Cho dù các TSFI sẽ là các cuộc gọi hệ thống hoặc API phụ thuộc vào những gì có sẵn cho ứng dụng: nếu các ứng dụng có thể sử dụng các cuộc gọi hệ thống trực tiếp, sau đó các cuộc gọi hệ thống là các TSFI. Tuy nhiên, nếu có một vài thứ ngăn cấm sử dụng trực tiếp của chúng và yêu cầu tất cả các truyền thông thông qua các API, sau đó các API sẽ là TSFI.

Một giao diện người dùng đồ họa tương tự: nó biên dịch giữa các lệnh máy dễ hiểu và đồ họa người dùng thân thiện. Tương tự, TSFI sẽ là các lệnh nếu người dùng có quyền truy cập tới chúng, hoặc các đồ họa (pull-down menu, kiểm tra hộp, các trường văn bản) nếu người sử dụng thường bị hạn chế sử dụng chúng.

Đáng chú ý là, trong cả hai ví dụ, nếu người dùng là bị cấm sử dụng các giao diện nguyên sơ (tức là các cuộc gọi hệ thống hay các lệnh), thì mô tả các hạn chế này và thực thi của nó sẽ được nêu trong các Mô tả Kiến trúc An toàn (xem A.1). Các wrapper cũng là một phần của TSF.

A.2.1.4 Các giao diện không được phép truy cập

Đối với một TOE đưa ra, không phải tất cả các giao diện có thể được truy cập. Đó là, các mục tiêu an toàn cho môi trường vận hành (trong Đích An toàn) có thể ngăn chặn việc truy cập vào các giao diện này hoặc giới hạn các truy cập trong một cách mà chúng không thể tiếp cận về mặt thực tế. Giao diện như vậy sẽ không được xem là TSFI. Một số ví dụ:

a) Nếu các mục tiêu an toàn cho môi trường vận hành đối với trạng thái stand-alone của tường lửa, nghĩa là trạng thái "tường lửa có thể là hoạt động trong một môi trường phòng máy chủ nơi mà chỉ nhân viên đáng tin cậy và được đào tạo có quyền truy cập, và sẽ được trang bị quyền có khả năng ngắt được việc cấp năng lượng (chống lại sự thất bại về năng lượng)", thì các giao diện vật lý và nguồn điện sẽ không thể truy cập được, vì một nhân viên đáng tin cậy và được đào tạo sẽ không cố gắng tháo dỡ tường lửa đó và/hoặc vô hiệu hóa nguồn cấp điện của nó.

b) Nếu các mục tiêu an toàn cho môi trường vận hành đối với trạng thái tường lửa phần mềm (ứng dụng), là trạng thái "hệ điều hành OS và phần cứng sẽ cung cấp một miền an toàn cho các ứng dụng tự do khỏi việc giả mạo của các chương trình khác", thì các giao diện mà qua đó tường lửa có thể được truy cập bởi các ứng dụng khác trên OS đó (ví dụ như xóa, sửa chữa

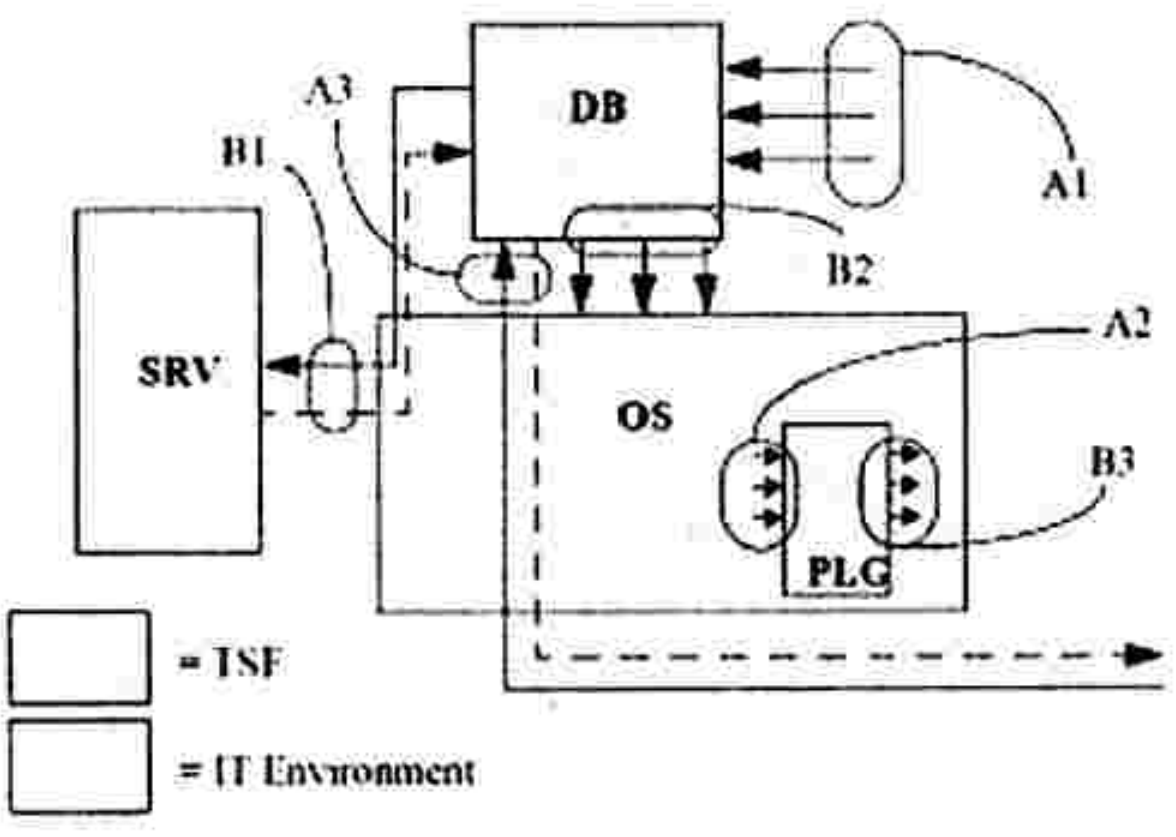
khả năng thực thi của tường lửa, đọc hoặc ghi trực tiếp vào không gian bộ nhớ của tường lửa) sẽ không thể truy cập được, vì bộ phận OS/phần cứng của môi trường vận hành đó khiến cho giao diện này không thể tiếp cận.

c) Nếu các mục tiêu an toàn cho môi trường vận hành đối với trạng thái tường lửa phần mềm bổ sung, trạng thái mà OS và phần cứng sẽ thực hiện chính xác các lệnh của TOE, và sẽ không can thiệp vào TOE theo bất kỳ cách nào, thì các giao diện mà qua đó tường lửa có được chức năng nguyên sơ từ OS và phần cứng (thực hiện các chỉ dẫn mã máy, hệ điều hành API, như tạo, đọc, ghi hoặc xóa các tập tin, các API đồ họa v.v...) sẽ không thể truy cập được, vì hệ điều hành / phần cứng là các thực thể duy nhất có thể truy cập vào giao diện, và chúng hoàn toàn đáng tin cậy.

Đối với tất cả các ví dụ này, các giao diện này không thể truy cập sẽ không thể là TSFI.

A.2.2 Ví dụ: một DBMS phức tạp

Hình A.2 minh họa một TOE phức tạp: một hệ thống quản lý cơ sở dữ liệu dựa trên phần cứng và phần mềm nằm ở bên ngoài ranh giới TOE (gọi tắt là môi trường CNTT trong phần còn lại của cuộc thảo luận này). Để đơn giản hóa ví dụ này, TOE là giống hệt với TSF. Các hộp tô màu sậm đại diện cho TSF, còn các hộp không tô màu đại diện cho các thực thể CNTT trong môi trường đó. TSF này bao gồm các công cụ và GUI quản lý cơ sở dữ liệu (đại diện bởi các hộp có nhãn DB) và mô-đun nhân chạy như một phần của hệ điều hành, thực hiện một số chức năng an toàn (đại diện bởi các hộp có nhãn PLG). Các mô-đun nhân TSF có các điểm nhập vào xác định bởi các đặc tả OS, cái mà OS sẽ viễn dẫn ra một số chức năng (điều này có thể là một trình điều khiển thiết bị, hoặc mô đune xác thực, vv.). Điều quan trọng là mô-đun nhân này có thể cắm nối này là cung cấp dịch vụ an toàn theo quy định của các yêu cầu chức năng trong ST này.



Hình A.2 – Các giao diện trong một hệ thống DBMS

Môi trường CNTT bao gồm các hệ điều hành của chính nó (thể hiện qua hộp có nhãn OS), cũng như các máy chủ bên ngoài (có tên là SRV). Máy chủ bên ngoài này, giống như OS, cung cấp một dịch vụ mà TSF phụ thuộc vào, và do đó cần phải được đặt trong môi trường CNTT. Giao diện trong hình được gắn nhãn Ax cho TSFI, và Bx cho các giao diện khác sẽ tài liệu hóa trong ACO là: Tổng hợp. Mỗi một nhóm các giao diện sẽ được thảo luận.

Giao diện nhóm A1 đại diện cho bộ rõ ràng nhất của TSFI. Đây là giao diện được sử dụng bởi người dùng truy cập trực tiếp cơ sở dữ liệu và chức năng và các tài nguyên an toàn của nó.

Giao diện A2 nhóm đại diện cho TSFI mà OS viện dẫn ra để đạt được những chức năng cung cấp bởi các module có thể cắm nối. Những giao diên này tương phản với nhóm giao diện B3, nhóm đại diện cho các cuộc gọi mà các module cắm nối tạo ra để đạt được các dịch vụ từ môi trường CNTT.

Giao diện nhóm A3 đại diện TSFI đi qua môi trường CNTT. Trong trường hợp này, các truyền thông DBMS qua mạng sử dụng một giao thức ở lớp ứng dụng. Trong khi môi trường CNTT có trách nhiệm cung cấp các giao thức hỗ trợ khác nhau (ví dụ, Ethernet, IP, TCP), giao thức lớp ứng dụng được sử dụng để đạt được các dịch vụ từ các DBMS, là một TSFI và phải được ghi nhận như vậy. Các đường chấm chấm biểu thị giá trị trả lại / dịch vụ từ các TSF qua kết nối mạng.

Các giao diện có nhãn Bx đại diện cho các giao diện đến các chức năng trong môi trường CNTT. Các giao diện này không phải là TSFI và chỉ cần được thảo luận và phân tích khi TOE đang được sử dụng trong một đánh giá tổng hợp như một phần của các hoạt động liên kết với các lớp ACO.

A.2.3 Ví dụ Đặc tả chức năng

Ví dụ tường lửa được sử dụng giữa một mạng nội bộ và mạng bên ngoài. Nó xác minh địa chỉ nguồn của các dữ liệu nhận được (để đảm bảo rằng dữ liệu bên ngoài không cố gắng giả mạo là có nguồn gốc từ các dữ liệu nội bộ), nếu nó phát hiện bất kỳ nỗ lực nào như vậy, nó sẽ giảm được sự tấn công vào các bản ghi kiểm toán. Các quản trị viên kết nối với tường lửa bằng cách thiết lập một kết nối telnet vào firewall từ các mạng nội bộ. Các hành động của quản trị viên bao gồm xác thực, thay đổi mật khẩu, xem xét các bản ghi kiểm toán, và thiết lập hoặc thay đổi địa chỉ của các mạng nội bộ và bên ngoài.

Ví dụ tường lửa đưa ra các giao diện sau đây với mạng nội bộ:

a) Các gói dữ liệu IP

b) Các lệnh nhà quản trị

và giao diện sau với mạng bên ngoài:

Các gói dữ liệu IP

Mô tả giao diện: Các gói dữ liệu IP

Các datagrams có định dạng theo quy định của RFC 791.

- Mục đích - để truyền tải các khối dữ liệu ("datagrams ") từ host nguồn đến host đích được xác định bởi chiều dài địa chỉ cố định; cũng cung cấp cho các phân mảnh và hợp mảnh của gói dữ liệu dài, nếu cần thiết, cho việc truyền thông qua các mạng gói nhỏ.
- Phương pháp sử dụng - chúng đến từ các giao thức lớp thấp hơn (ví dụ như liên kết dữ liệu).
- Tham số - gồm các trường sau của tiêu đề gói tin IP: địa chỉ nguồn, đích đến địa chỉ, cờ không phân mảnh.
- Mô tả các thông số - [Như được định nghĩa bởi RFC 791, mục 3.1 ("Định dạng tiêu đề mạng")]
- Hành động - Truyền gói dữ liệu mà không phải là giả mạo; phân mảnh các gói dữ liệu lớn nếu cần thiết; lắp ghép các mảnh thành các gói dữ liệu.
- Bản tin báo lỗi - (không có). Không có các gói tin không thể phân phát (ví dụ như phải được phân mảnh để truyền, nhưng cờ không phân mảnh được thiết lập) được đảm bảo độ tin cậy (độ tin cậy để được cung cấp bởi các giao thức lớp trên) bị mất.

Giao diện mô tả: Các lệnh quản trị

Các lệnh quản trị cung cấp một phương tiện cho người quản trị tương tác với các tường lửa. Những lệnh và sự đáp lại này đi trên kết nối telnet (RFC 854) được thiết lập từ bất kỳ host nào trong mạng nội bộ. Các lệnh sẵn có là:

- **Passwd**
  - Mục đích - đặt mật khẩu quản trị
  - Phương pháp Sử dụng - **passwd <mật khẩu>**
  - Thông số - mật khẩu
  - Mô tả thông số - giá trị của mật khẩu mới
  - Hành động - thay đổi mật khẩu để thêm giá trị mới. Không có giới hạn.
  - Bản tin báo lỗi - không có.
- **Readaudit**
  - Mục đích - trình bày các bản ghi kiểm toán cho các quản trị viên
  - Phương pháp sử dụng - **Readaudit**
  - Thông số - không có
  - Mô tả thông số - không
  - Hành động – cung cấp các văn bản của các bản ghi kiểm toán
  - Thông báo lỗi - không có.
- **Setintaddr**
  - Mục đích – tập địa chỉ của các địa chỉ nội bộ
  - Phương pháp sử dụng - **Setintaddr** <địa chỉ>
  - Tham số - địa chỉ
  - Mô tả tham số - ba trường đầu tiên của một địa chỉ IP (được định nghĩa trong RFC 791). Ví dụ: 123.123.123
  - Hành động - thay đổi giá trị nội bộ của biến số xác định mạng nội bộ, giá trị này của nó được sử dụng để phân định sự giả mạo
  - Thông báo lỗi - "địa chỉ được sử dụng": chỉ ra mạng nội bộ được đã định danh là giống như các mạng bên ngoài
- **Setextaddr**
  - Mục đích - bộ địa chỉ của địa chỉ bên ngoài
  - Phương pháp sử dụng – **Setextaddr** <địa chỉ>
  - Tham số - địa chỉ
  - Mô tả tham số - ba trường đầu tiên của một địa chỉ IP (như được định nghĩa trong RFC 791). Ví dụ: 123.123.123
  - Hành động - thay đổi giá trị nội bộ của biến xác định các mạng bên ngoài

- Thông báo lỗi - "địa chỉ được sử dụng": chỉ ra mạng bên ngoài được định danh giống như các mạng nội bộ

A.3 ADV_INT: Tài liệu bổ sung trên TSF nội bộ

Sự đa dạng của các TOE làm cho nó không thể hệ thống hóa bất cứ cái gì xác định hơn "có cấu trúc" hay "phức tạp tối thiểu". Sự phán đoán trên cấu trúc và tính phức tạp được dự kiến sẽ xuất phát từ các công nghệ cụ thể sử dụng trong các TOE. Ví dụ, phần mềm có thể được xem xét cấu trúc tốt khi nó biểu lộ đặc điểm được trích dẫn trong các ngành kỹ thuật phần mềm.

Phụ lục này cung cấp tài liệu bổ sung về việc đánh giá cấu trúc và sự phức tạp của các thành phần phần mềm thủ tục cơ sở của TSF. Tài liệu này dựa trên các thông tin có sẵn trong các tài liệu kỹ thuật phần mềm. Đối với các loại khác của TSF nội bộ (ví dụ như phần cứng, không phần mềm không thủ tục như mã hướng đối tượng, vv), tương ứng với tài liệu để thực hành tốt nên được tư vấn.

A.3.1 Cấu trúc phần mềm thủ tục

Cấu trúc của phần mềm thủ tục được đánh giá truyền thống theo mô đun của nó. Phần mềm được viết với sự hỗ trợ của thiết kế mô-đun trong việc đạt được sự dễ hiểu bằng cách làm rõ các mối phụ thuộc nào mà một module có trên các module khác (khớp nối) và nêu rõ các nhiệm vụ chỉ trong một module là có liên quan rõ rệt với nhau (gắn kết). Việc sử dụng các thiết kế mô đun làm giảm các mối phụ thuộc lẫn nhau giữa các phần tử của TSF và do đó làm giảm rủi ro mà sự thay đổi hoặc lỗi trong một module sẽ có ảnh hưởng trong suốt TOE. Việc sử dụng của nó tăng cường độ rõ nét của thiết kế và cung cấp sự đảm bảo cao, nghĩa là các tác động không mong đợi sẽ không xảy ra. Các thuộc tính mong muốn của sự phân tách mô-đun là giảm số lượng mã dư thừa hoặc không cần thiết.

Giảm thiểu số lượng các chức năng trong TSF cho phép các thẩm định viên cũng như các nhà phát triển chỉ tập trung vào các chức năng nào cần thiết cho SFR thực thi, giúp dễ hiểu hơn và tiếp tục hạ thấp khả năng các lỗi thiết kế hoặc thực hiện.

Sự hợp nhất của việc phân tách, xếp lớp và hạn chế tối đa mô đun vào quá trình thiết kế và thực thi phải được đi kèm với những cân nhắc kỹ thuật phần mềm âm thanh. Một hệ thống phần mềm thực tế, hữu ích thường sẽ kéo theo một số khớp nối không mong muốn giữa các module, một số mô-đun bao gồm các chức năng liên kết rời rạc, và một số lại tinh vi hoặc phức tạp trong thiết kế của một module. Những sai lệch so với những lý tưởng của sự phân tách mô đun thường được coi là cần thiết để đạt được một số mục tiêu hoặc hạn chế, có thể là liên quan đến hiệu năng, tính tương thích, chức năng lên kế hoạch trong tương lai, hoặc một số yếu tố khác, và có thể chấp nhận được, dựa trên sự điều chỉnh của nhà phát triển cho chúng. Khi áp dụng các yêu cầu của lớp này, vì việc xem xét phải đưa đến nguyên tắc kỹ thuật phần mềm âm thanh, tuy nhiên, mục tiêu tổng thể của tính dễ hiểu phải đạt được.

A.3.1.1 Sự gắn kết

Sự gắn kết là cách thức và mức độ mà ở đó các nhiệm vụ được thực hiện bởi một module phần mềm đơn nhất, có liên quan với sự gắn kết khác; các loại gắn kết bao gồm sự trùng khớp, khả năng truyền thông, chức năng, logic, tuần tự, và về thời gian. Những loại gắn kết được đặc trưng dưới đây, được liệt kê theo thứ tự giảm dần về mong muốn.

a) gắn kết về chức năng - một module với gắn kết về chức năng thực hiện các hoạt động liên quan đến một mục đích đơn nhất. Một module gắn kết về chức năng chuyển đổi một loại đầu vào đơn của thành một loại đầu ra đơn, cũng như một quản lý ngăn xếp hoặc một quản lý một hàng đợi.

b) gắn kết tuần tự - một mô-đun gắn kết tuần tự chứa mỗi chức năng của có đầu ra của nó là đầu vào cho các chức năng theo sau trong module. Một ví dụ về một mô-đun gắn kết tuần tự là một

mô đun trong đó chứa các chức năng ghi hồ sơ kiểm toán và duy trì hoạt động đếm của số tích lũy của các hành vi vi phạm kiểm toán theo một loại cụ thể.

c) gắn kết truyền thông - một mô-đun gắn kết truyền thông chứa những chức năng mà tạo ra đầu ra, hoặc sử dụng đầu ra từ, các chức năng khác trong module. Một ví dụ về mô-đun gắn kết truyền thông là một mô đun iểm tra truy cập bao gồm kiêm tra bắt buộc, tùy ý, và năng lực.

d) gắn kết về thời gian – chứa các chức năng cần thiết để thực hiện tại cùng một thời điểm. Ví dụ về các mô-đun gắn kết bao gồm khởi động, phục hồi, và các mô-đun tắt máy.

e) gắn kết về logic (hoặc thủ tục) - một mô-đun với sự gắn kết về logic sẽ thực các hiện hoạt động tương tự nhau trên cấu trúc dữ liệu khác nhau. Một cuộc mô-đun trình bày sự gắn kết về logic nếu các chức năng của nó thực hiện các hoạt động liên quan, nhưng khác nhau trên các đầu vào khác nhau.

f) gắn kết trùng khớp - một mô-đun với gắn kết trùng khớp thực hiện các hoạt động ngẫu nhiên không liên quan, hoặc liên quan lỏng lẻo.

A.3.1.2 Ghép nối

Ghép nối là cách thức và mức độ phụ thuộc lẫn nhau giữa các module phần mềm; các loại khớp nối bao gồm nối cuộc gọi, chung và nội dung. Các loại khớp nối được miêu tả dưới đây, liệt kê theo thứ tự mong muốn giảm dần:

a) lời gọi: hai mô-đun được gọi cùng nếu chúng truyền thông chặt chẽ thông qua việc sử dụng các cuộc gọi chức năng được viện dẫn của chúng, ví dụ về khớp nối gọi là dữ liệu, nhãn hiệu, và kiểm soát, được định nghĩa dưới đây.

1) dữ liệu: hai mô-đun được khớp nối dữ liệu nếu chúng truyền thông chặt chẽ thông qua việc sử dụng các thông số cuộc gọi dữ liệu duy nhất đại diện cho các mục dữ liệu.

2) nhãn hiệu: hai mô-đun được khớp nối nhãn hiệu nếu chúng giao tiếp thông qua việc sử dụng các thông số cuộc gọi mà bao gồm nhiều trường hoặc có cấu trúc có ý nghĩa nội bộ.

3) Kiểm soát: hai mô-đun được khớp nối điều khiển nếu một mô đun vượt qua thông tin được dùng để gây ảnh hưởng đến logic nội bộ của nhau.

b) chung: hai mô-đun được khớp nối chung nếu chúng chia sẻ một vùng dữ liệu chung hoặc một tài nguyên hệ thống chung. Biến chung chỉ ra rằng các mô-đun bằng cách sử dụng các biến chung được ghép nối chung. Khớp nối chung thông qua các biến chung thường được cho phép, nhưng chỉ đến một mức độ hạn chế. Ví dụ, các biến được đặt vào một khu vực toàn cầu, nhưng được sử dụng chỉ bởi một module đơn nhất, và được đặt không thích hợp, và nên xóa bỏ. Các yếu tố khác cần được xem xét trong đánh giá phù hợp của các biến chung là:

1) Một số mô đun thay đổi biến toàn cầu: Nói chung, chỉ có một mô-đun duy nhất nên được giao trách nhiệm cho việc kiểm soát các nội dung của một biến toàn cầu, nhưng có thể có các tình huống trong đó một mô-đun thứ hai có thể chia sẻ trách nhiệm đó, trong trường hợp đó, lý lẽ bào chữa đầy đủ phải được cung cấp. Không chấp nhận trách nhiệm này cho việc chia sẻ bởi nhiều hơn hai mô-đun. (Trong việc đánh giá này, điều quan tâm nên được đưa ra để xác định mô-đun thực sự chịu trách nhiệm về nội dung của biến, ví dụ, nếu một thường trình đơn nhất được sử dụng để sửa đổi các biến, nhưng thường trình đó chỉ đơn giản thực hiện việc sửa đổi theo yêu cầu của người gọi của nó, thì đó là module gọi có trách nhiệm, và có thể có nhiều hơn một mô đun như vậy). Hơn nữa, như một phần của việc xác định phức tạp, nếu hai module chịu trách nhiệm về nội dung của một biến toàn cầu, cần có chỉ dẫn rõ ràng về cách sửa đổi được điều phối giữa chúng.

2) Một số mô đun tham chiếu một biến toàn cầu: Mặc dù nói chung không có giới hạn về số lượng các module tham chiếu một biến toàn cầu, các trường hợp trong đó nhiều mô-đun thực hiện như một tham chiếu thì nên được kiểm tra về tính hợp lệ và cần thiết.

c) nội dung: Hai mô-đun được ghép nối nội dung nếu một mô đun có thể tham chiếu trực tiếp vào bên trong của mô đun kia (vi dụ sửa đổi mã của mô đun còn lại, hoặc tham chiếu nhãn nội bộ tới các module còn lại). Kết quả là một số hoặc tất cả các nội dung của một module được chứa một cách có hiệu quả trong việc mô đun kia. Khớp nối nội dung có thể được dùng như cách sử dụng giao diện mô đun không quảng bá, điều này trái ngược với cuộc gọi ghép đôi, chỉ sử dụng giao diện module quảng bá.

A.3.2 Tính phức tạp của phần mềm thủ tục

Phức tạp là biện pháp điểm quyết định và tuyến logic của việc thực hiện mà các mã đưa ra. tài liệu kỹ thuật phần mềm trích dẫn sự phức tạp như là một đặc tính tiêu cực của phần mềm bởi vì nó cản trở tính thông minh về sự logic và flow của mã đó. Một trở ngại khác cho sự thông minh của mã là sự hiện diện của những mã không cần thiết, mà ở đó nó không được sử dụng hoặc thừa.

Việc sử dụng cách phân lớp để chia thành các mức độ trừu tượng và giảm thiểu phụ thuộc vòng tròn hơn nữa cho phép một sự hiểu biết tốt hơn về TSF, cung cấp sự bảo đảm hơn, điều mà các yêu cầu chức năng an toàn TOE chính xác và hoàn toàn được thuyết minh trong việc thực thi.

Giảm sự phức tạp cũng bao gồm việc giảm hoặc loại bỏ các mối phụ thuộc lẫn nhau, mà gắn liền cả hai với mô-đun trong một lớp đơn nhất và để chúng trong các lớp riêng biệt. Module phụ thuộc lẫn nhau có thể dựa vào nhau để xây dựng một kết quả duy nhất, mà có thể dẫn đến một tình trạng bế tắc, hoặc tệ hơn, một điều kiện tranh đua (ví dụ, thời gian kiểm tra so với thời gian quan tâm sử dụng), nơi mà các kết luận cuối cùng có thể không xác định được và lệ thuộc vào môi trường điện toán tại thời điểm được đưa ra tức thì.

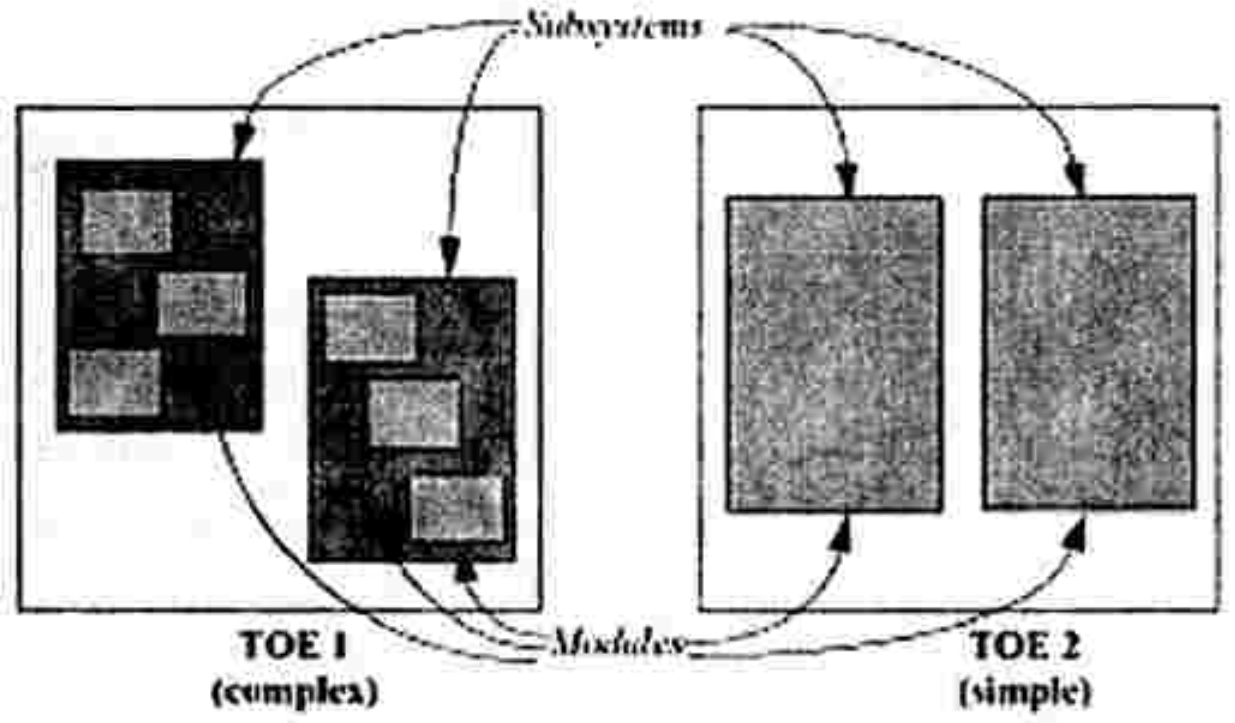
Giảm thiểu sự phức tạp của thiết kế là một đặc tính quan trọng của một cơ chế xác nhận tính hợp lệ của sự tham chiếu, mục đích của nó là để đi đến việc dễ dàng hiểu một TSF để nó có thể được phân tích hoàn toàn. (Có những đặc điểm quan trọng khác của một cơ chế xác tính hợp lệ tham chiếu, như TSF tự bảo vệ và non-bypassability; các đặc tính khác được bao trùm bởi các yêu cầu trong họ ADV_ARC.)

A.4 ADV_TDS: Các hệ thống con và mô đun

Mục này cung cấp hướng dẫn bổ sung về họ TDS, và cách sử dụng của nó trong thuật ngữ "hệ thống con" và "mô đun". Tiếp theo là một thảo luận về cách có nhiều chi tiết được thêm thế nào, yêu cầu đối với một số chi tiết được giảm như thế nào.

A.4.1 Các hệ thống con

Hình A.3 cho thấy rằng, việc phụ thuộc vào sự phức tạp của TSF, thiết kế có thể được mô tả trong phạm vi hệ thống con và các mô-đun (nơi mà các hệ thống con có một mức độ trừu tượng cao hơn so với các mô-đun), hoặc nó chỉ có thể được mô tả trong phạm vi của một mức độ trừu tượng (ví dụ, các hệ thống con ở các cấp độ đảm bảo thấp hơn, mô-đun ở các cấp cao hơn). Trong trường hợp mức trừu tượng thấp hơn (modules) được trình bày, các yêu cầu đánh vào cấp trừu tượng (các hệ thống con) được về cơ bản đáp ứng theo mặc định. Khái niệm này là tiếp tục xây dựng trong các cuộc thảo luận về các hệ thống con và các module dưới đây.



Hình A.3 – Các hệ thống con và các mô đun

Nhà phát triển được trông đợi mô tả việc thiết kế các TOE trong phạm vi của hệ thống con. Thuật ngữ "hệ thống con" đã được lựa chọn không rõ ràng để nó có thể tham khảo các khối phù hợp với TOE (ví dụ, các hệ thống con, mô-đun). Các hệ thống con thậm chí có thể không đồng đều trong phạm vi, miễn là các yêu cầu về mô tả của các hệ thống con được đáp ứng.

Việc sử dụng đầu tiên của các hệ thống con là để phân biệt ranh giới TSF, đó là, các phần của TOE đó bao gồm các TSF. Nói chung, một hệ thống con là một phần của TSF nếu nó có khả năng (dù theo thiết kế hoặc thực thi) để ảnh hưởng đến các hoạt động chính xác của bất kỳ SFR. Ví dụ, đối với phần mềm phụ thuộc vào phương thức thực hiện phần cứng khác nhau để đưa ra sự phân tách miền (xem A.1) nơi mã SFT thực thi được thực hiện trong một miền, sau đó tất cả các hệ thống con mà thực hiện ở miền đó có thể coi là một phần của TSF. Tương tự như vậy, nếu một máy chủ bên ngoài miền đó thực thi một SFR (ví dụ như thi hành một chính sách kiểm soát truy cập đối với các đối tượng nó được quản lý), thì sau đó nó cũng sẽ được coi là một phần của TSF.

Việc sử dụng thứ hai của các hệ thống con là cung cấp một cấu trúc để mô tả các TSF ở một mức độ mô tả đó, trong việc mô tả cách TSF làm việc thế nào, không nhất thiết phải bao gồm chi tiết thực hiện ở mức thấp được tìm thấy trong các mô tả module (thảo luận sau). Các hệ thống con này được mô tả ở hoặc ở một cấp độ cao (thiếu đa dạng về chi tiết thi hành) hoặc ở một cấp độ chi tiết (cung cấp cái nhìn sâu hơn trong việc thi hành). Cấp độ mô tả cung cấp cho một hệ thống con được xác định bởi mức độ mà hệ thống con đó có trách nhiệm thi hành một SFR.

Một hệ thống con SFR-thực thi là một hệ thống con cung cấp cơ chế để thi hành một phần tử của SFR bất kỳ, hoặc trực tiếp hỗ trợ một hệ thống con có trách nhiệm thi hành một SFR. Nếu một hệ thống con cung cấp (các thực thi) một TSFI SFR-thực thi, thì sau đó hệ thống con là SFR thực thi.

Các hệ thống con cũng có thể được xác định là SFR hỗ trợ và SFR không can thiệp. Một hệ thống con SFR hỗ trợ là một hệ thống bị phụ thuộc bởi một hệ thống con SFR thực thi, để thi hành SFR, nhưng không có vai trò trực tiếp như một hệ thống con SFR thực thi. Một hệ thống con SFR không can thiệp là một hệ thống trong đó không bị phụ thuộc vào cả hai vai trò hỗ trợ hoặc thực thi, để thi hành một SFR.

A.4.2 Các mô đun

Module tổng quan là một khối kiến trúc tương đối nhỏ có thể được đặc trưng trong giới hạn các thuộc tính được thảo luận trong nội bộ TSF (ADV_INT). Khi cả hai yêu cầu thiết kế mô-đun cơ bản ADV_TDS.3 (hoặc ở trên) và yêu cầu nội bộ TSF (ADV_INT) có mặt trong một PP hoặc ST, thì một "module" trong giới hạn các yêu cầu thiết kế TOE (ADV_TDS) đề cập đến cùng một thực thể như là

một "module" cho yêu cầu nội bộ TSF (ADV_INT). Không giống như các hệ thống con, module mô tả việc thực thi ở một mức độ chi tiết có thể phục vụ như một hướng dẫn để xem xét các đại diện thực thi.

Điều quan trọng cần lưu ý rằng, tùy thuộc vào TOE, các mô-đun và các hệ thống con có thể đề cập đến cùng sự trừu tượng. Đối với thiết kế cơ bản ADV_TDS.1 và thiết kế kiến trúc ADV_TDS.2 (mà không yêu cầu mô tả ở cấp module), mô tả hệ thống con cung cấp các chi tiết mức thấp nhất sẵn có về các TSF. Đối với thiết kế mô-đun cơ bản ADV_TDS.3 (mà yêu cầu mô tả module), thì những mô tả này cung cấp mức thấp nhất của chi tiết, trong khi mô tả hệ thống con (nếu chúng tồn tại như những thực thể riêng biệt) chỉ đơn thuần phục vụ cho việc đưa vào các mô tả module. Đó là, nó không nhất thiết để cung cấp các mô tả hệ thống con chi tiết nếu mô tả module tồn tại. Trong các TOE đơn giản, một "mô tả hệ thống con" riêng biệt là không cần thiết; các yêu cầu có thể được đáp ứng thông qua các tài liệu được cung cấp bởi mô-đun. Đối với các TOE phức tạp, mục đích của các mô tả hệ thống con (đối với các TSF) là cung cấp cho người đọc bối cảnh để họ có thể tập trung vào những phân tích của họ một cách thích hợp. Sự khác biệt này được minh họa trong Hình A.3.

Một mô đun SFR- thực thi là một mô-đun trực tiếp thi hành một yêu cầu chức năng an toàn(SFR) trong ST. Mô-đun như vậy thường sẽ thi hành một TSFI SFR-thực thi, nhưng một số chức năng thể hiện trong một SFR (ví dụ đối với kiểm toán và các chức năng tái sử dụng đối tượng) có thể không trực tiếp gắn liền với một TSFI đơn nhất. Như trường hợp với các hệ thống con, module SFR hỗ trợ là những module bị phụ thuộc bởi module SFR thực thi, nhưng không chịu trách nhiệm trực tiếp thi hành một SFR. Các mô đun SFR không can thiệp là những module mà không xử lý, trực tiếp hoặc gián tiếp, với việc thi hành SFR.

Điều quan trọng cần lưu ý rằng việc xác định "thực thi trực tiếp" nào có nghĩa là hơi chủ quan. Trong nghĩa hẹp của thuật ngữ, nó có thể được giải thích theo nghĩa một hoặc hai đường của mã thực sự thực hiện một so sánh, hoạt động zeroing, v.v... mà thi hành một yêu cầu. Một giải thích rộng hơn có thể bao gồm các module viện dẫn ra để trả lời một TSFI SFR thực thi, và tất cả các mô-đun có thể được gọi lần lượt bởi module đó (và như vậy cho đến khi hoàn thành cuộc gọi). Cả hai giải thích đó đều không đặc biệt đáp ứng, vì theo nghĩa hẹp của sự giải thích đầu tiên có thể dẫn đến các module quan trọng không được phân loại chính xác như SFR hỗ trợ, và thứ hai là dẫn đến các mô đun thực sự không phải SFR thực thi đang được phân loại như vậy.

Một mô tả của một module nên được như vậy để người ta có thể tạo ra một thực thi của các mô-đun từ mô tả, và việc thực thi kết quả sẽ là 1) trùng với việc thực thi TSF thực tế trong giới hạn các giao diện trình bày và sử dụng bởi mô-đun, và 2) thuật toán giống với các module TSF. Ví dụ, RFC 793 cung cấp một mô tả cấp cao của giao thức TCP. Nó nhất thiết sự độc lập trong thực thi. Trong khi nó cung cấp rất nhiều chi tiết, thì nó không phải là một mô tả thiết kế phù hợp bởi vì nó không cụ thể cho một thực thi. Một thực thi thực tế có thể thêm vào các giao thức được quy định trong RFC, và sự lựa chọn thực thi (ví dụ, việc sử dụng các dữ liệu toàn cầu so với dữ liệu cục bộ ở nhiều phần thực thi) có thể có tác động tới các phân tích đang thực hiện. Mô tả thiết kế của module TCP sẽ lập nên danh sách các giao diện trình bày sự thực thi (thay vì chỉ những cái được định nghĩa trong RFC 793), cũng như một mô tả thuật toán xử lý các liên kết với các mô-đun thực thi TCP (Giả sử họ là một phần của TSF).

Trong thiết kế, mô-đun mô tả chi tiết trong giới hạn chức năng mà chúng cung cấp (mục đích); các giao diện chúng trình bày, các giá trị trở về từ các giao diện như vậy, các giao diện (được trình bày bởi các module khác) mà chúng sử dụng, và một mô tả về cách chúng cung cấp chức năng của mình (một cách có thể cho mô tả các chức năng là một mô tả thuật toán).

Mục đích của một module nên được mô tả thấy được chức nào mà module cung cấp. Nó nên đầy đủ để người đọc có thể nắm bắt được một ý tưởng chung của những chức năng của mô-đun trong kiến trúc.

Các giao diện trình bày của một module là những giao diện được sử dụng bởi các module khác để viện dẫn chức năng cung cấp. Giao diện bao gồm cả giao diện hiện (ví dụ, một trình tự gọi viện dẫn bởi các mô đun khác) cũng như các giao diện ẩn (ví dụ dữ liệu toàn cầu thao tác bởi module). Giao diện này được mô tả trong giới hạn chúng được viện dẫn thế nào, và bất kỳ giá trị được trả về. Mô tả này sẽ bao gồm một danh sách các thông số, và những mô tả về các thông số này. Nếu một tham số được dự kiến sẽ đưa vào một tập hợp các giá trị (ví dụ, một tham số " cờ"), thì việc thiết lập đầy đủ các giá trị của tham số đó có thể đảm nhận, sẽ tác dụng trên mô đun đang trong tiến trình được chỉ định. Tương tự như vậy, các thông số đại diện cho cấu trúc dữ liệu được mô tả tới mức mỗi trường của cấu trúc dữ liệu cũng được xác định và mô tả. Dữ liệu toàn cầu nên được mô tả như dù là nó được đọc hoặc ghi (hoặc cả hai) bởi module.

Lưu ý rằng ngôn ngữ lập trình khác nhau có thể có thêm các "giao diện" mà có thể không rõ ràng; chẳng hạn sẽ là người vận hành/chức năng quá tải trong C++. " giao diện ẩn " này trong mô tả lớp cũng sẽ được mô tả như là một phần của thiết kế mô-đun. Lưu ý rằng mặc dù một module có thể chỉ trình bày một giao diện, nó phổ biến hơn là một mô-đun trình bày một tập hợp nhỏ các giao diện liên quan.

Ngược lại, giao diện sử dụng bởi các module phải được nhận biết rõ để nó có thể xác định được module nào đang được viện dẫn bởi mô đun được mô tả. Cần phải rõ ràng từ mô tả thiết kế, sở cứ thuật toán học, mô đun đang được viễn dẫn ra. Ví dụ, nếu Module A được mô tả, và nó sử dụng thường trình sắp xếp bubble của Module B, thì một mô tả thuật toán không đầy đủ sẽ là "Module A viện dẫn ra giao diện double_bubble () trong Module B để thực hiện một sắp xếp bubble". Một mô tả thuật toán đầy đủ sẽ là "Module A viện dẫn ra thường trình double_bubble với danh sách các mục điều khiển truy cập; double_bubble () sẽ trả về các mục được sắp xếp đầu tiên là tên người dùng, sau đó là trường access_allowed theo quy tắc sau đây ..." Mô tả chi tiết của một module trong thiết kế phải cung cấp đủ chi tiết để thấy rõ được tác dụng nào mà Module A là mong đợi từ giao diện sắp xếp bubble. Lưu ý rằng một trong những phương pháp trình bày này được gọi là các giao diên thông qua một cây cuộc gọi, và khi đó mô tả thuật toán có thể được bao gồm trong mô tả thuật toán của các module gọi.

Như đã thảo luận trước, mô tả thuật toán của module nên mô tả một cách thuật toán thực thi các module. Điều này có thể được thực hiện trong mã giả, thông qua các biểu đồ dòng chảy, hoặc (ADV_TDS.3 thiết kế mô-đun cơ bản) dạng văn bản. Nó bản về cách thức các đầu vào mô-đun và các chức năng gọi được sử dụng để hoàn thành chức năng của module. Nó ghi chú sự thay đổi dữ liệu toàn cầu, trạng thái hệ thống, và các giá trị trả lại được tạo bởi module. Đó là ở cấp độ chi tiết mà một thực thi có thể phát sinh, có thể rất giống với một thực thi thực tế của TOE.

Cần lưu ý rằng mã nguồn không đáp ứng yêu cầu tài liệu minh chứng mô-đun. Mặc dù thiết kế module mô tả việc thực thi đó, nhưng nó không phải là một thực thi. Các ý kiến xung quanh các mã nguồn có thể là tài liệu minh chứng đầy đủ nếu chúng cung cấp một lời giải thích về mục đích của mã nguồn.

Trong các phần tử dưới đây, các nhãn (SFR thực thi, SFR hỗ trợ, và SFR không can thiệp) được thảo luận đối với các hệ thống con và các mô-đun được sử dụng để mô tả số lượng và loại thông tin cần tạo sẵn bởi nhà phát triển. Các phần tử đã được cấu trúc như vậy là để không có kỳ vọng để các nhà phát triển cung cấp chỉ thông tin được quy định. Đó là, nếu tài liệu minh chứng của TSF của nhà phát triển cung cấp các thông tin trong các yêu cầu dưới đây, không có kỳ vọng rằng các nhà phát triển cập nhật tài liệu minh chứng của họ và các hệ thống con và mô-đun nhãn như SFR thực thi, SFR hỗ trợ, và SFR không can thiệp. Mục đích chính của việc gán nhãn này là cho phép các nhà phát triển với những phương pháp phát triển chưa hoàn thiện (và hiện vật liên quan, chẳng hạn như giao diện chi tiết và tài liệu minh chứng thiết kế) cung cấp bằng chứng cần thiết mà không cần chi phí quá mức.

A.4.3 Phương thức phân mức

Bảng A.1 – Mô tả phân mức chi tiết

	Hệ thống con TSF			Mô đun TSF		
	Thực thi SFR	Hỗ trợ SFR	SFR NI	Thực thi SFR	Hỗ trợ SFR	SFR NI
ADV_TDS.1 Thiết kế cơ bản (trình bày không chính thức)	Cấu trúc, tóm tắt hoạt động thực thi SFR và tương tác	Hỗ trợ thiết kế (1)	Hỗ trợ thiết kế			
ADV_TDS.2 Thiết kế kiến trúc (trình bày không chính thức)	Cấu trúc, tóm tắt hoạt động thực thi SFR và tương tác	Cấu trúc, tóm tắt hoạt động thực thi SFR và tương tác	Hỗ trợ thiết kế			
ADV_TDS.3 Thiết kế mô đun cơ bản (trình bày không chính thức)	Mô tả, tương tác	Mô tả, tương tác	Mô tả, tương tác	Mục đích, các giao diện SFR (2)	Tương tác, mục đích	Tương tác, mục đích
ADV_TDS.4 Thiết kế mô đun bán chính thức (trình bày bán chính thức)	Mô tả, tương tác	Mô tả, tương tác	Mô tả, tương tác	Mục đích, các giao diện SFR	Mục đích, các giao diện SFR	Tương tác, mục đích
ADV_TDS.5 Thiết kế mô đun bán chính thức đầy đủ (trình bày bán chính thức)	Mô tả, tương tác	Mô tả, tương tác	Mô tả, tương tác	Mục đích, mọi giao diện (3)	Mục đích, mọi giao diện	Mục đích, mọi giao diện
ADV_TDS.6 Thiết kế mô đun bán chính thức đầy đủ với trình bày thiết kế mức cao chính thức (trình bày bán chính thức; trình bày chính thức bổ sung)	Mô tả, tương tác	Mô tả, tương tác	Mô tả, tương tác	Mục đích, mọi giao diện	Mục đích, mọi giao diện	Mục đích, mọi giao diện

(1) *Hỗ trợ thiết kế:* nghĩa là chỉ cần các tài liệu đủ cho hỗ trợ phân loại hệ thống con / mô đun.

(2) *Giao diện SFR:* nghĩa là mô tả mô đun có chứa các giá trị trả về và các giao diện được gọi tới các mô đun khác cho mỗi giao diện liên quan SFR.

(3) *Mọi giao diện:* nghĩa là mô tả mô đun có chứa các giá trị trả về và các giao diện được gọi tới các mô đun khác cho mỗi giao diện.

Bởi vì có tính chủ quan trong việc xác định cái nào là SFR thực thi với SFRhỗ trợ (và trong một số trường hợp, thậm chí xác định cái nào là SFR không can thiệp) các mô hình sau đây đã được áp dụng trong họ này. Trong phần đầu của họ, nhà phát triển tạo ra một quyết định về việc phân loại các hệ thống con thành SFR thực thi, v.v..., cung cấp các thông tin thích hợp, và có một số bằng chứng bổ sung cho các thẩm định viên xem xét để hỗ trợ tuyên bố này. Vì mức độ đảm bảo mong muốn gia tăng,

trong khi nhà phát triển vẫn tạo một quyết định phân loại, thì thẩm định viên có được càng nhiều bằng chứng được sử dụng để xác nhận việc phân loại của nhà phát triển.

Để tập trung phân tích các đánh giá thẩm định viên trên các phần SFR liên quan của TOE, đặc biệt là ở cấp đảm bảo thấp hơn, các thành phần của họ được phân mức để thông tin chi tiết ban đầu được yêu cầu chỉ cho các thực thể kiến trúc SFR thực thi. Vì mức độ đảm bảo gia tăng, nên nhiều thông tin được yêu cầu cho SFR hỗ trợ và (cuối cùng) các thực thể SFR-không can thiệp. Cần lưu ý rằng ngay cả khi thông tin đầy đủ được yêu cầu, thì nó cũng không được yêu cầu để tất cả các thông tin này được phân tích trong cùng một mức độ chi tiết. Trong mọi trường hợp nên tập trung vào việc liệu các thông tin cần thiết đã được cung cấp và phân tích.

Bảng A.1 tóm tắt các thông tin yêu cầu tại mỗi của những thành phần họ đối với các thực thể kiến trúc được mô tả.

A.5 Tài liệu bổ trợ về phương pháp chính thức

Phương pháp chính quy cung cấp sự trình bày về toán học của TSF và cách xử lý của nó và được yêu cầu bởi ADV_FSP.6 Đặc tả chức năng bán chính thức đầy đủ, ADV_SPM.1 mô hình chính sách an toàn TOE chính thức, và ADV_TDS.6 thiết kế mô-đun chính thức đầy đủ với các thành phần trình bày thiết kế cấp cao chính quy. Có hai khía cạnh của phương pháp chính quy: ngôn ngữ đặc tả được sử dụng để biểu thị chính thức, và định lý chứng minh để chứng minh sự đầy đủ và chính xác về toán học của các đặc tả chính thức.

Một đặc tả chính thức được thể hiện trong một hệ thống dựa trên các khái niệm toán học đã được xác minh. Những khái niệm toán học này được sử dụng để xác định rõ ràng ngữ nghĩa, cú pháp và các quy tắc của suy luận. Một hệ thống chính quy là một hệ thống nhận dạng và mối quan hệ trừu tượng có thể được mô tả bằng cách chỉ định một bảng chữ cái chính thức, một ngôn ngữ chính thức trên bảng chữ cái dựa trên một cú pháp chính thức, và một tập quy tắc chính thức của suy luận cho việc xây dựng các dẫn xuất của câu trong ngôn ngữ chính quy.

Các thẩm định viên phải kiểm tra việc hệ thống chính quy nhận dạng để đảm bảo rằng:

- Các quy tắc ngữ nghĩa, cú pháp và suy luận của hệ thống chính quy được định nghĩa hay định nghĩa được tham chiếu
- Mỗi hệ thống chính quy có kèm theo văn bản giải thích để cung cấp nghĩa ngữ được đinh nghĩa sao cho
    1) các văn bản giải thích đưa ra ý nghĩa được định nghĩa của các từ ngữ, chữ viết tắt và từ viết tắt được sử dụng trong một ngữ cảnh khác được chấp nhận sử dụng bình thường;
    2) việc sử dụng một hệ thống chính thức và sử dụng ký hiệu bán chính thức được đi kèm bằng cách hỗ trợ văn bản giải thích theo cách thức phù hợp với ý nghĩa rõ ràng;
    3) hệ thống chính thức có thể thể hiện các quy tắc và đặc điểm của SFP áp dụng, chức năng bảo mật và các giao diện (quy định chi tiết các hiệu ứng, ngoại lệ và thông báo lỗi) của TSF, hệ thống phụ hoặc các mô-đun của chúng được chỉ định cho các họ đảm bảo với ký hiệu được sử dụng;
    4) ký hiệu cung cấp các quy tắc để xác định ý nghĩa của các cấu trúc cú pháp hợp lệ.
- Mỗi hệ thống chính thức sử dụng một cú pháp chính thức cung cấp các quy tắc để nhận ra các cấu trúc rõ ràng.
- Mỗi hệ thống các quy tắc chính thức cung cấp bằng chứng mà

5) hỗ trợ lý luận hợp lý của các khái niệm toán học thiết lập tốt,

6) giúp ngăn chặn nguồn gốc của mâu thuẫn.

Nếu nhà phát triển sử dụng một hệ thống chính thức mà đã được chấp nhận bởi cơ quan đánh giá, thẩm định viên có thể dựa vào mức độ hình thức và sức mạnh của hệ thống và tập trung vào các thuyết minh của hệ thống chính thức cho các đặc tả TOE và chứng minh thư.

Cách thức chính quy hỗ trợ chứng minh toán học của tài sản bảo đảm dựa trên các tính năng bảo mật, tính thống nhất của các sàng lọc và thư từ của các cơ quan đại diện.

Ví dụ về các hệ thống chính thức:

- Ngôn ngữ đặc tả Z là có ý, và hỗ trợ nhiều phương pháp khác nhau hoặc phong cách của đặc tả kỹ thuật chính thức
- Việc sử dụng Z đã được chủ yếu cho các đặc điểm kỹ thuật theo định hướng mô hình, sử dụng lược đồ để chính thức chỉ định hoạt động. Xem http://vl.zuser.org/.
- ACL2 là một mã nguồn mở chính thức hệ thống bao gồm một ngôn ngữ dựa trên đặc điểm kỹ thuật LISP và Prover một định lý. Xem http://www.cs.utexas.edu/users/moore/acl2/ cho biết thêm thông tin.
- Isabelle là một định lý chung phổ biến chứng minh môi trường cho phép các công thức toán học được thể hiện bằng một ngôn ngữ chính thức và cung cấp công cụ để chứng minh những công thức trong một tính toán hợp lý (http://www.cl.cam.ac.uk/Research/ HVG / Isabelle /).
- Phương pháp B là một hệ thống chính thức dựa trên các phép tính mệnh đề, các phép tính đơn hàng đầu tiên vị với các quy tắc suy luận và lý thuyết tập hợp (ví dụ http://vl.fmnet.info/b/).

Phụ lục B

(Quy định)

Tổng hợp (ACO)

Mục tiêu của phụ lục này là để giải thích các khái niệm đằng sau đánh giá tổng hợp và các tiêu chuẩn ACO. Phụ lục này không định nghĩa các tiêu chí ASE; định nghĩa này có thể được tìm thấy tại mục 10.

B.1 Sự cần thiết đối với các đánh giá TOE tổng hợp

Thị trường CNTT được tạo thành từ sự cung cấp một loại hình sản phẩm / công nghệ của nhà cung cấp. Mặc dù có một số loại hình chồng lấn nhau, khi mà một nhà cung cấp phần cứng máy tính cũng có thể cung cấp phần mềm ứng dụng và / hoặc hệ điều hành hoặc nhà sản xuất chip cũng có thể phát triển một hệ điều hành dành riêng cho các chipset của chính họ, thường thấy đó là trường hợp một giải pháp CNTT được thực hiện bởi nhiều nhà cung cấp khác nhau.

Đôi khi cần phải đảm bảo trong sự kết hợp (sự tổng hợp) của các thành phần ngoài sự đảm bảo của các thành phần riêng lẻ. Mặc dù có sự hợp tác giữa các nhà cung cấp, trong việc phổ biến của vật chất nhất định cần thiết cho việc tích hợp kỹ thuật của các thành phần, các thỏa thuận hiếm khi kéo dài đến mức cung cấp thông tin thiết kế chi tiết và quá trình phát triển / thủ tục bằng chứng. Việc thiếu thông tin từ nhà phát triển về một thành phần mà thành phần khác phụ thuộc, có nghĩa là các nhà phát triển thành phần phụ thuộc không có quyền truy cập vào các loại thông tin cần thiết để thực hiện một đánh giá của cả hai thành phần phụ thuộc và cơ sở tại EAL2 hoặc cao hơn. Vì vậy, trong khi một đánh giá của các thành phần phụ thuộc vẫn có thể được thực hiện ở bất cứ cấp đảm bảo nào, để soạn các thành phần với bảo đảm tại EAL2 hoặc ở trên, nó là cần thiết để tái sử dụng các bằng chứng và kết quả đánh giá đánh giá được thực hiện đối với các nhà phát triển thành phần.

Điều mong đợi là các tiêu chí ACO có thể áp dụng trong hoàn cảnh mà một thực thể IT phụ thuộc vào thực thể IT khác để cung cấp các dịch vụ an toàn. Các thực thể cung cấp các dịch vụ được gọi là, "thành phần cơ sở", và nhận các dịch vụ được gọi là, "thành phần phụ thuộc". Mối quan hệ này có thể tồn tại trong một số ngữ cảnh. Ví dụ, một ứng dụng (thành phần phụ thuộc) có thể sử dụng dịch vụ được cung cấp bởi một hệ điều hành (thành phần cơ sở). Ngoài ra, mối quan hệ có thể là peer-to-peer, trong ý nghĩa của hai ứng dụng liên kết, hoặc là đang chạy trong một môi trường hệ điều hành phổ biến, hoặc trên các nền tảng phần cứng riêng biệt. Nếu có một đồng đẳng chi phối cung cấp các dịch vụ cho các đồng đẳng thứ yếu, thì các đồng đẳng chi phối được coi là thành phần cơ sở và đồng đẳng thứ yếu là thành phần phụ thuộc. Nếu các đồng đẳng cung cấp dịch vụ với nhau theo một cách thức chung nhau, mỗi đồng đẳng sẽ được coi là thành phần cơ sở cho các dịch vụ được cung cấp và thành phần phụ thuộc cho các dịch vụ được yêu cầu. Điều này đòi hỏi sự lặp lại của những thành phần ACO áp dụng tất cả các yêu cầu với từng loại thành phần đồng đẳng.

Các tiêu chí này cũng dự định sẽ được áp dụng rộng rãi hơn, từng bước (nơi một TOE tổng hợp bao gồm một thành phần phụ thuộc và một thành phần cơ sở mà bản thân nó đã trở thành một thành phần cơ sở của một TOE tổng hợp khác), trong nhiều mối quan hệ phức tạp, nhưng điều này có thể yêu cầu giải thích thêm.

Điều cần thiết các đánh giá TOE tổng hợp là các thành phần riêng rẽ được đánh giá độc lập, vì việc đánh giá tổng hợp xây dựng dựa trên các kết quả đánh giá thành phần riêng rẽ. Việc đánh giá của các thành phần phụ thuộc có thể vẫn đang được tiến hành khi bắt đầu đánh giá TOE tổng hợp. Tuy nhiên, việc đánh giá thành phần phụ thuộc phải hoàn thành trước khi đánh giá TOE tổng hợp hoàn tất.

Các hoạt động đánh giá tổng hợp có thể diễn ra đồng thời với đánh giá thành phần phụ thuộc. Điều này là do hai yếu tố:

a) Những bộ phận điều khiển về kinh tế/thương mại - nhà phát triển thành phần phụ thuộc hoặc là sẽ tài trợ cho các hoạt động đánh giá tổng hợp hoặc hỗ trợ các hoạt động này như các đánh giá phân rã từ việc đánh giá thành phần phụ thuộc được yêu cầu cho hoạt động đánh giá tổng hợp.

b) Những bộ phận điều khiển về kỹ thuật - các thành phần xem xét liệu việc bảo đảm cần thiết có được cung cấp bởi các thành phần cơ sở (ví dụ như xem xét các thay đổi trong thành phần cơ sở kể từ khi hoàn thành việc đánh giá thành phần) với sự hiểu biết về các thành phần phụ thuộc gần đây đã trải qua (đang trải qua) đánh giá thành phần và tất cả các đánh giá phân rã được kết hợp với đánh giá sẵn có. Vì vậy, không có các hoạt động trong khi tổng hợp, khi tổng hợp đó có yêu cầu các hoạt động đánh giá thành phần phụ thuộc phải được thẩm tra lại. Ngoài ra, nó được thẩm tra rằng các thành phần cơ sở tạo thành (một trong) các cấu hình kiểm thử cho việc kiểm thử các thành phần phụ thuộc trong việc đánh giá thành phần phụ thuộc, để lại ACO_CTT để xem xét các thành phần cơ sở trong cấu hình này.

Các bằng chứng đánh giá từ việc đánh giá các thành phần phụ thuộc là yêu cầu đầu vào cho các hoạt động đánh giá TOE tổng hợp. Chỉ các tài liệu đánh giá từ việc đánh giá của các thành phần cơ sở mà được yêu cầu như là đầu vào cho các hoạt động đánh giá TOE tổng hợp:

a) Các điểm yếu dư trong thành phần cơ sở, được báo cáo trong quá trình đánh giá thành phần cơ sở. Điều này được yêu cầu cho các hoạt động ACO_VUL.

Không có bằng chứng đánh giá khác từ thành phần cơ sở các hoạt động nên được yêu cầu cho việc đánh giá TOE tổng hợp, khi đó kết quả đánh giá từ việc đánh giá thành phần của các thành phần cơ sở nên được sử dụng lại. Thông tin thêm về các thành phần cơ sở có thể được yêu cầu nếu các TOE tổng hợp TSF gồm nhiều thành phần cơ sở hơn đã được xem xét là TSF trong các đánh giá thành phần của các thành phần cơ sở.

Việc đánh giá thành phần của các thành phần cơ sở và phụ thuộc được giả định là hoàn thành vào thời gian phán quyết cuối cùng được giao cho các thành phần ACO.

Các thành phần ACO_VUL chỉ xem xét sức bền chống lại kẻ tấn công với một cuộc tấn công tiềm ẩn lên đến Cơ bản được nâng cao. Điều này là do mức độ thông tin thiết kế cho biết cách thành phần cơ sở cung cấp các dịch vụ mà ở đó các thành phần phụ thuộc dựa vào như thế nào thông qua các ứng dụng của các hoạt động ACO_DEV. Do đó, tinh bí mật phát sinh từ đánh giá TOE tổng hợp sử dụng CAP được giới hạn trong một mức độ tương tự như thu được từ đánh giá TOE thành phần EAL4. Mặc dù bảo đảm trong các thành phần đó bao gồm các TOE tổng hợp có thể cạo hơn EAL4.

B.2 Thực hiện đánh giá Mục tiêu An toàn đánh giá đối với một TOE tổng hợp

Một ST sẽ được đệ trình bởi nhà phát triển cho việc đánh giá các TOE tổng hợp (thành phần cơ sở + thành phần phụ thuộc). ST này sẽ xác định các gói đảm bảo được áp dụng cho các TOE tổng hợp, cung cấp sự bảo đảm trong thực thể được tổng hợp bằng cách lấy ra khi sự đảm bảo đã đạt được trong các đánh giá thành phần.

Mục đích của việc xem xét sự tổng hợp của các thành phần trong ST một là để xác nhận sự phù hợp của các thành phần từ điểm nhìn của cả môi trường và các yêu cầu, và cũng để đánh giá rằng các ST TOE tổng hợp là phù hợp với các ST thành phần và chính sách an toàn thể hiện trong chúng. Điều này bao gồm việc xác định rằng các ST thành phần và chính sách an toàn thể hiện trong đó là tương thích.

Các ST TOE tổng hợp có thể nhắc đến bên ngoài nội dung của ST thành phần, hoặc tác giả ST có thể chọn để nhắc lại những tài liệu của ST thành phần bên trong ST TOE tổng hợp cung cấp một sở cứ về ST thành phần được thể hiện trong ST TOE tổng hợp như thế nào.

Trong việc thực hiện các hoạt động đánh giá ASE_CCL cho một ST TOE tổng hợp, nhà đánh giá xác định rằng các ST thành phần là đại diện chính xác trong các ST TOE tổng hợp. Điều này đạt được thông qua việc xác định rằng các ST TOE tổng hợp phù hợp với các ST TOE thành phần. Ngoài ra, các nhà đánh giá sẽ cần phải xác định rằng sự phụ thuộc của các thành phần phụ thuộc trên môi trường hoạt động được đáp ứng đầy đủ trong TOE tổng hợp.

Mô tả TOE tổng hợp sẽ mô tả giải pháp được tổng hợp. Phạm vi logic và vật lý và ranh giới của giải pháp tổng hợp sẽ được mô tả, và (các) ranh giới về logic giữa các thành phần cũng sẽ được xác định. Những mô tả này sẽ xác định các chức năng an toàn được cung cấp bởi mỗi thành phần.

Tuyên bố của các SFR đối với TOE tổng hợp sẽ xác định được thành phần nào là thỏa mãn một SFR. Nếu một SFR được đáp ứng bởi cả hai thành phần, thì tuyên bố đó sẽ xác định được thành phần nào đáp ứng các khía cạnh khác nhau của SFR. Tương tự, Đặc điểm Tóm tắt TOE tổng hợp sẽ xác định thành phần nào cung cấp chức năng an toàn được mô tả.

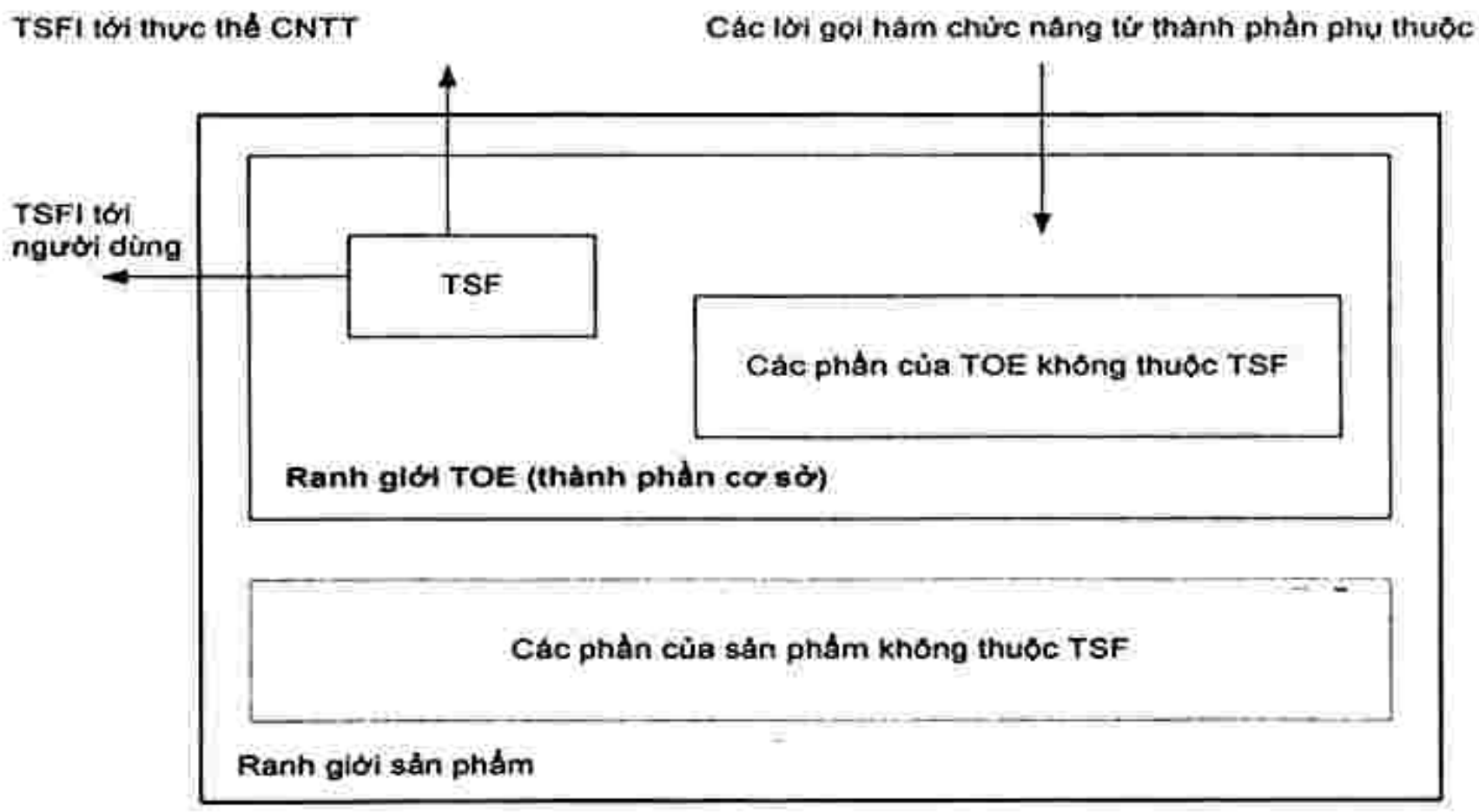
Các gói của ASE: các yêu cầu đánh giá Mục tiêu An toàn áp dụng cho các ST TOE tổng hợp nên nhất quán với các gói của ASE: các yêu cầu đánh giá Mục tiêu An toàn được sử dụng trong các đánh giá thành phần.

Tái sử dụng kết quả đánh giá từ đánh giá của các ST thành phần có thể được thực hiện trong các trường hợp mà các ST TOE tổng hợp trực tiếp đề cập đến các ST thành phần, ví dụ: nếu ST TOE tổng hợp đề cập đến một ST thành phần đối với một phần tuyên bố của SFR của nó, nhà đánh giá có thể hiểu rằng các yêu cầu cho việc hoàn thành tất cả các hoạt động chỉ định và lựa chọn (như đã nêu trong ASE_REQ .*. 3C) đã được thỏa mãn trong các đánh giá thành phần .

B.3 Các tương tác giữa các thực thể CNTT tổng hợp

Các TSF của thành phần cơ sở thường được xác định mà không biết về sự phụ thuộc của các ứng dụng có thể có mà nó có thể có nhờ được tổng hợp. Các TSF của thành phần cơ sở này được định nghĩa bao gồm tất cả các bộ phận của các thành phần cơ sở, là các thành phần phải dựa vào thực thi của SFR thành phần cơ sở. Điều này sẽ bao gồm tất cả các bộ phận của các thành phần cơ sở được yêu cầu để thực thi các SFR thành phần cơ sở.

TSFI của thành phần cơ sở này đại diện cho các giao diện được cung cấp bởi các TSF đối với các thực thể bên ngoài, các thực thể này đã được được định nghĩa trong tuyên bố của SFR để gọi một dịch vụ của TSF. Điều này bao gồm các giao diện cho người sử dụng thuộc về con người và cũng có giao diện cho các thực thể CNTT bên ngoài. Tuy nhiên, TSFI chỉ bao gồm những giao diện cho các TSF, và do đó không nhất thiết phải là một đặc tả giao diện đầy đủ của tất cả các giao diện có thể có giữa một thực thể bên ngoài và thành phần cơ sở. Thành phần cơ sở có thể trình bày các giao diện cho các dịch vụ không được coi là an toàn-có liên quan, hoặc vì mục đích vốn có của các dịch vụ (ví dụ, điều chỉnh phông chữ) hoặc bởi vì SFR theo tiêu chuẩn ISO / IEC 15408 liên quan, không được tuyên bố trong ST của các thành phần cơ sở (ví dụ như giao diện đăng nhập khi không có FIA theo tiêu chuẩn ISO / IEC 15408-2: SFR Định danh và xác thực được xác nhận).



Hình B.1 – Trừu tượng hóa thành phần cơ sở

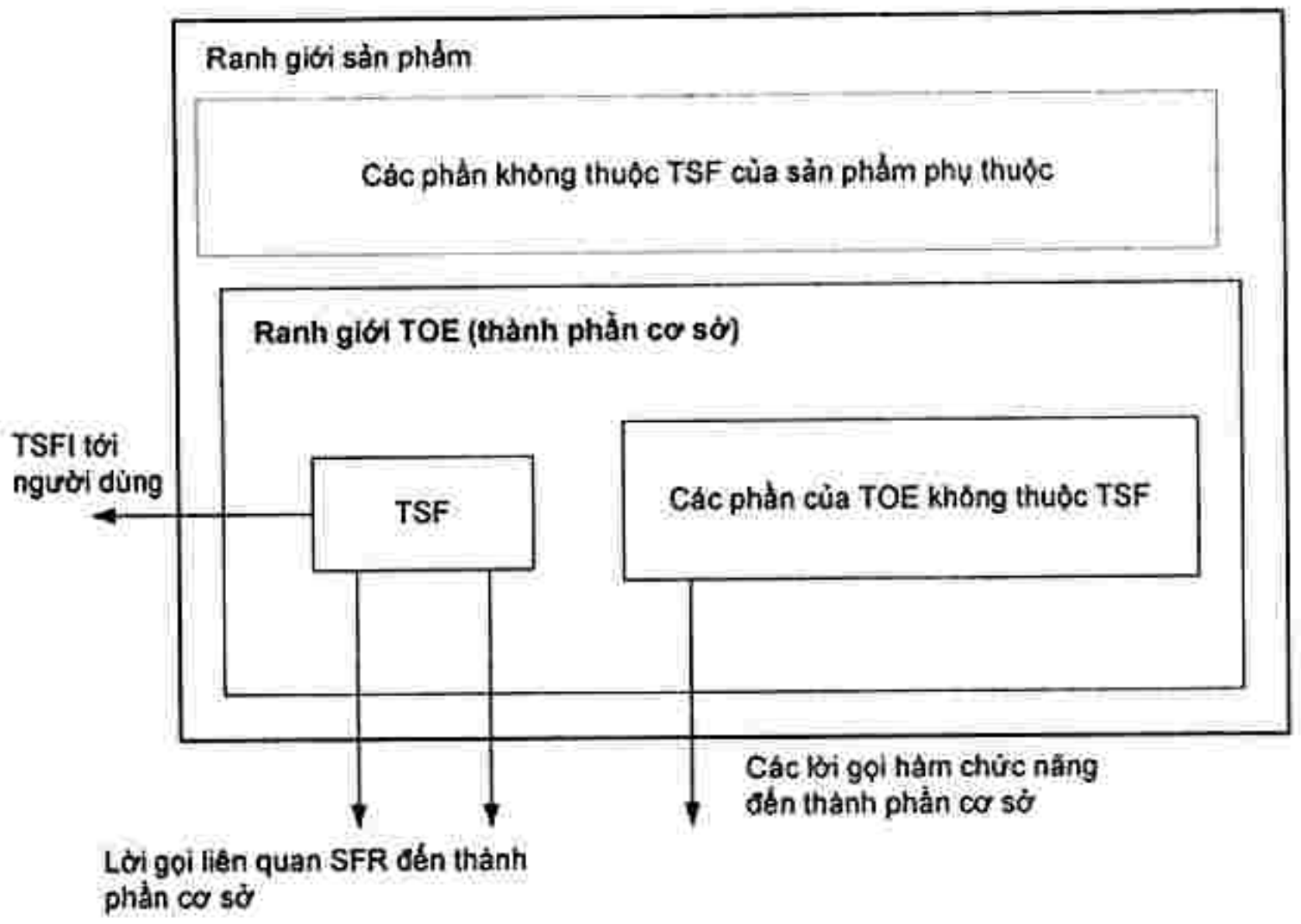
Các giao diện chức năng cung cấp bởi các thành phần cơ sở nằm ngoài các giao diện an toàn (TSFIs), và không cần phải được xem xét trong quá trình đánh giá thành phần cơ sở. Những giao diện này thường bao gồm các giao diện được sử dụng bởi một thành phần phụ thuộc để viện dẫn một dịch vụ được cung cấp bởi các thành phần cơ sở.

Các thành phần cơ sở có thể bao gồm một số các giao diện gián tiếp thông qua đó TSFIs có thể được gọi, ví dụ: các API có thể được dùng để viện dẫn một dịch vụ của TSF, mà không được xem xét trong đánh giá của các thành phần cơ sở.

Các thành phần phụ thuộc, dựa vào các thành phần cơ sở, được xác định tương tự: giao diện cho các thực thể bên ngoài định nghĩa trong các SFR của ST thành phần được phân loại như TSFI và được kiểm tra trong ADV_FSP.

Bất kỳ cuộc gọi ra từ các TSF phụ thuộc tới môi trường hỗ trợ của một SFR sẽ cho thấy các TSF phụ thuộc yêu cầu một số dịch vụ từ môi trường để đáp ứng việc thực thi của các SFR thành phần phụ thuộc. Như một dịch vụ nằm ngoài ranh giới thành phần phụ thuộc và các thành phần cơ sở là không được quy định tại các ST phụ thuộc như là một thực thể bên ngoài. Do đó, các cuộc gọi cho các dịch vụ được thực hiện bởi các TSF phụ thuộc đến nền tảng cơ bản của nó (các thành phần cơ sở) sẽ không được phân tích như là một phần của hoạt động cácđặc tả chức năng (ADV_FSP). Những phụ thuộc dựa vào thành phần cơ sở này được thể hiện trong ST thành phần phụ thuộc như mục tiêu an toàn cho môi trường.

Sự trừu tượng này của các thành phần và các giao diện phụ thuộc được hiển thị trong Hình B.2 dưới đây.

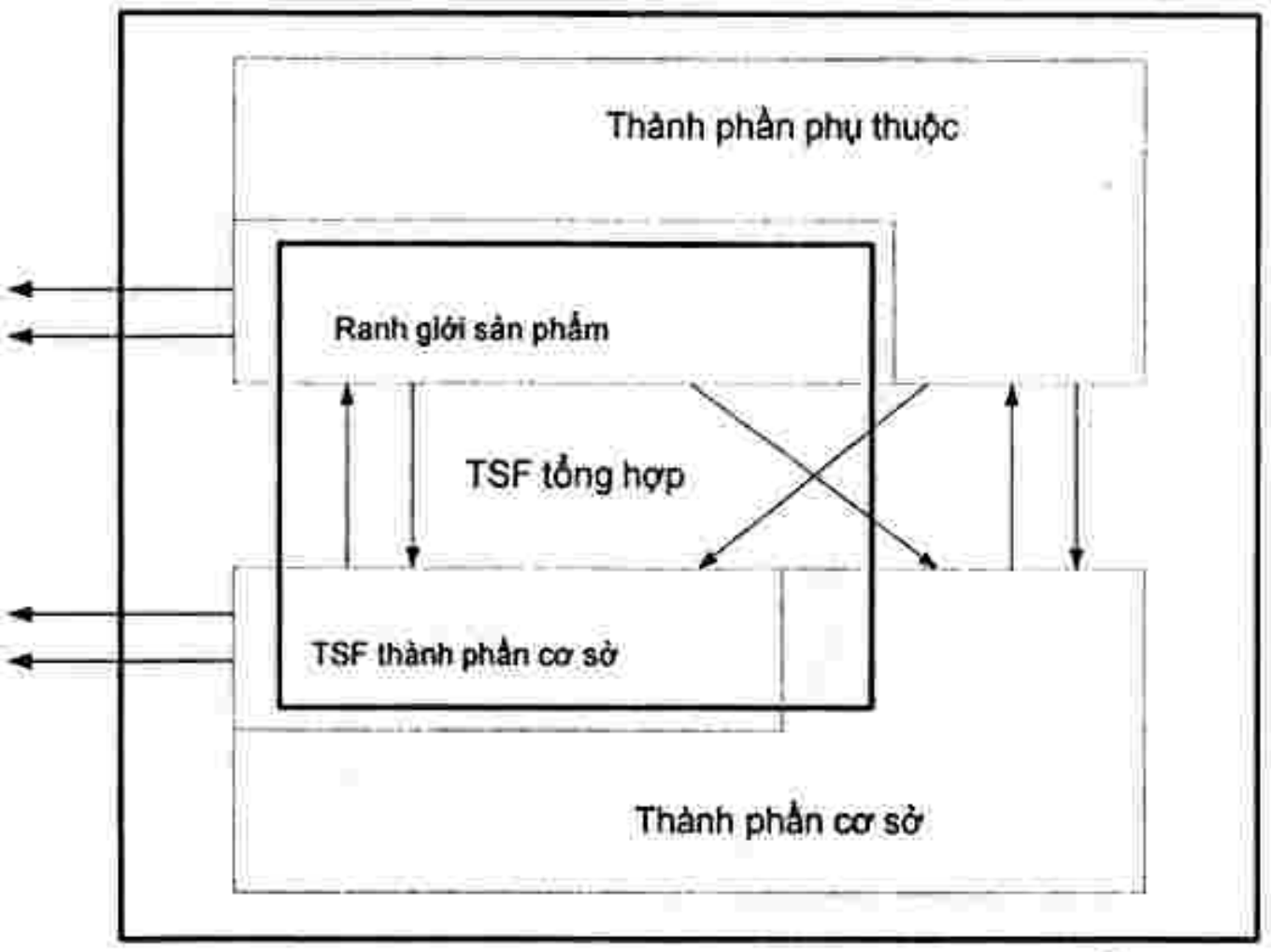


Hình B.2 – Trừu tượng hóa thành phần phụ thuộc

Khi xem xét các thành phần của các thành phần cơ sở và thành phần phụ thuộc, nếu các thành phần phụ thuộc của TSF yêu cầu dịch vụ từ các thành phần cơ sở để hỗ trợ việc thực thi của SFR, thì giao diện cho dịch vụ sẽ cần phải được định nghĩa. Nếu dịch vụ được cung cấp bởi TSF của thành phần cơ sở, thì giao diện đó nên là một TSFI của thành phần cơ sở và do đó sẽ được xác định trong đặc tả chức năng của thành phần cơ sở.

Tuy nhiên, nếu dịch vụ được gọi là bởi TSF của thành phần phụ thuộc không được cung cấp bởi TSF của thành phần cơ sở (tức là, nó được thực thi trong các phần không phải TSF của thành phần cơ sở hoặc có thể ngay cả trong những phần không phải TOE của các thành phần cơ sở (không minh họa trong Hình B.3), không thể xảy ra là một TSFI của thành phần cơ sở liên quan đến dịch vụ đó, trừ các dịch vụ là trung gian của TSF của thành phần cơ sở. Các giao diện cho các dịch vụ này từ các thành phần phụ thuộc đến môi trường hoạt động được xem xét trong họ Sự tin cậy của các thành phần phụ thuộc (ACO_REL).

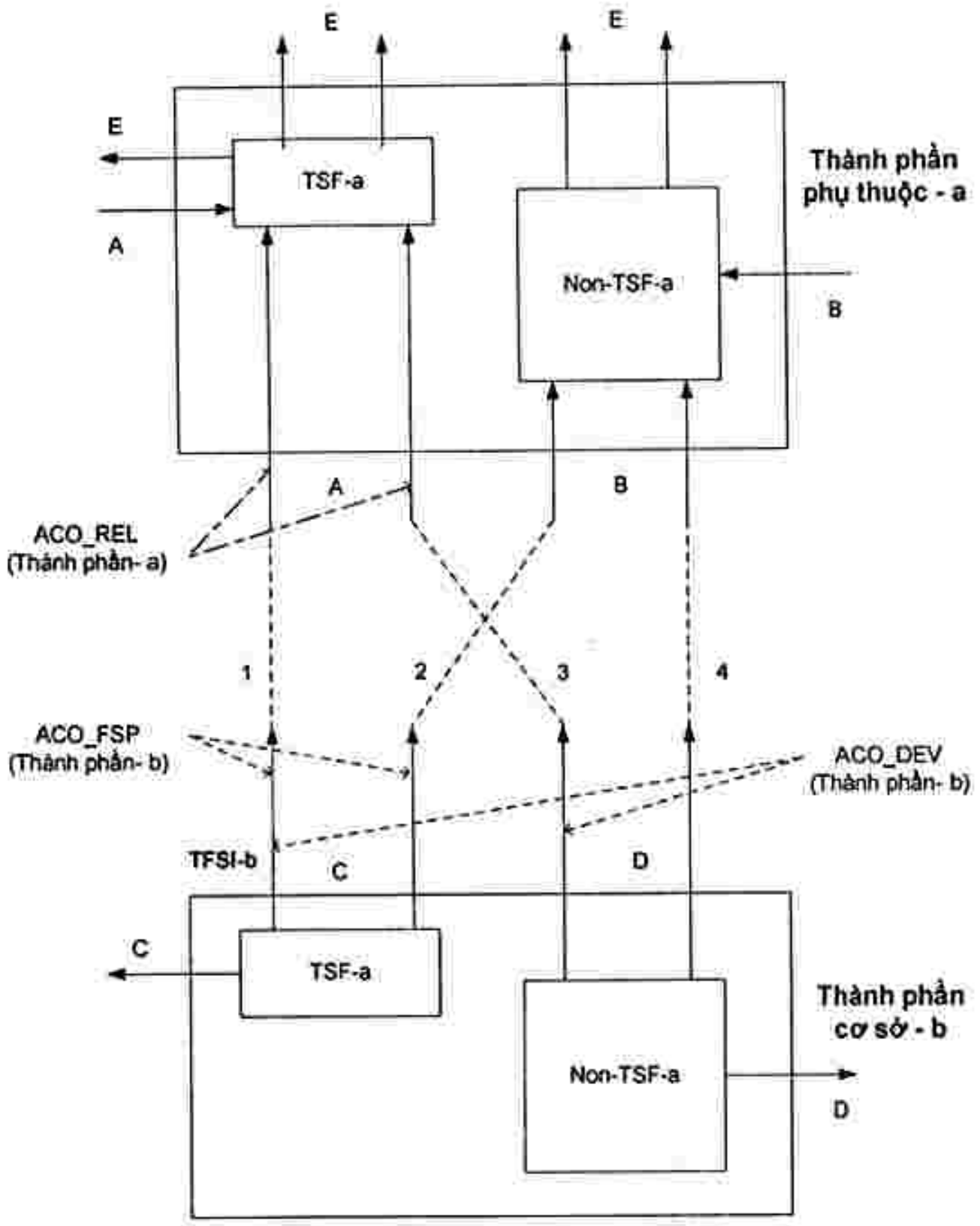
Các phần không phải-TSF của thành phần cơ sở được lấy vào trong TSF của TOE được tổng hợp do các sự phụ thuộc các thành phần phụ thuộc có trên thành phần cơ sở để hỗ trợ các SFR của thành phần phụ thuộc. Do vậy, trong trường hợp này, TSF của TOE tổng hợp lớn hơn tổng số các của các TSF của thành phần.



Hình B.3 – Trừu tượng hóa TOE tổng hợp

Có thể là trường hợp, các thành phần cơ sở TSFI được gọi một cách không lường trước trong việc đánh giá thành phần cơ sở. Do đó sẽ có một yêu cầu cho việc thử nghiệm xa hơn của thành phần cơ sở TSFI.

Các giao diện có thể được tiếp tục được mô tả trong sơ đồ (Hình B.4) và văn bản hỗ trợ sau.



Hình B.4 – Các giao diện thành phần cơ sở

(1) Các mũi tên đi vào " thành phần phụ thuộc-a '(A và B) = nơi thành phần mong đợi môi trường đáp ứng một yêu cầu dịch vụ (trả lời các cuộc gọi ra từ các thành phần phụ thuộc vào môi trường);

(2) Các mũi tên ra khỏi "thành phần cơ sở-b '(C và D) = các giao diện của các dịch vụ cung cấp bởi thành phần cơ sở cho môi trường;

(3) đường gạch chấm giữa các thành phần = các loại thông tin liên lạc giữa các cặp của các giao diện;

(4) Các mũi tên (màu xám) còn lại = các giao diện được mô tả bởi các tiêu chí nhất định.

Sau đây là một trường hợp đơn giản, nhưng giải thích những yếu tố cần được thực hiện.

Có thành phần một ('thành phần phụ thuộc-a') và b ('thành phần cơ sở-b'): các mũi tên ra khỏi TSF-a là các dịch vụ cung cấp bởi TSF-a và do đó là TSFI (a); tương tự, các mũi tên ra khỏi TSF-b ("C") là TSFI (b). Thành phần a là để yêu cầu các dịch vụ từ môi trường của nó: chúng cần TSF (a) được gắn nhãn "A", còn dịch vụ kia (không liên quan đến TSF-a) được gắn nhãn "B".

Khi thành phần-a và thành phần-b được kết hợp, có bốn tổ hợp có thể có của {dịch vụ cần thiết bởi thành phần-a} và {dịch vụ được cung cấp bởi thành phần-b}, hiển thị như các đường đứt nét (các loại hình truyền thông giữa các cặp của các giao diện). Bất kỳ tập hợp nào của chúng đều có thể tồn tại cho một tổng hợp cụ thể:

a) TSF-a yêu cầu các dịch vụ được cung cấp bởi TSF-b ("A" được kết nối với "C"): trường hợp đơn giản: các chi tiết về "C" được đặt ở FSP cho thành phần-b. Trong trường hợp này các giao diện nên được định nghĩa trong đặc tả chức năng cho thành phần-b.

b) Non-TSF-a yêu cầu các dịch vụ được cung cấp bởi TSF-b ("B" được kết nối với "C"): trường hợp đơn giản (lặp lại, các chi tiết về "C" được đặt ở FSP cho thành phần-b) , nhưng không quan trọng: an toàn khôn ngoan.

c) Non-TSF-a yêu cầu các dịch vụ được cung cấp bởi non-TSF-b ("B" được kết nối với "D"): chúng ta không có thông tin chi tiết về D, nhưng không có sự liên quan an toàn về việc sử dụng các giao diện này , vì vậy chúng không cần phải được xem xét trong đánh giá, mặc dù chúng có thể sẽ là một vấn đề hội nhập cho các nhà phát triển.

d) TSF-a yêu cầu các dịch vụ được cung cấp bởi không-TSF-b ("A" được kết nối với "D"): điều này sẽ xuất hiện khi thành phần-a và thành phần-b có nghĩa khác nhau về những gì một "dịch vụ bảo vệ" được. Có lẽ b-là thành phần làm cho không có tuyên bố về I & A (không có SFR FIA trong ST của nó), nhưng thành phần cần chứng thực được cung cấp bởi môi trường của nó. Không có thông tin chi tiết về "D" giao diện có sẵn (họ không TSFI (b), vì vậy chúng không có trong thành phần FSP-b này).

Lưu ý: nếu các loại tương tác được mô tả trong trường hợp d trên tồn tại, sau đó là TSF của TOE sáng tác sẽ được TSF-a + TSF-b + Non-TSF-b. Nếu không, TSF của TOE sáng tác sẽ được TSF-a + TSF-b.

Giao diện loại 2 và 4 của Hình B.4 không trực tiếp liên quan đến việc thẩm định gồm TOE. Giao diện 1 và 3 sẽ được xem xét trong quá trình ứng dụng của các gia đình khác nhau:

a) đặc tả chức năng (ADV_FSP) (cho thành phần-b) sẽ mô tả các giao diện C.
b) Sự tin cậy của các thành phần phụ thuộc (ACO_REL) sẽ mô tả các giao diện A.
c) Bằng chứng phát triển (ACO_DEV) sẽ mô tả các giao diện C cho kết nối loại 1 và các D giao diện cho kết nối loại 3.

Một ví dụ điển hình mà thành phần có thể được áp dụng là một hệ thống quản lý cơ sở dữ liệu (DBMS) dựa vào hệ điều hành cơ bản của nó (OS). Trong đánh giá của các thành phần DBMS, sẽ có một đánh giá tạo nên từ các thuộc tính an toàn của DBMS đó (đến bất cứ độ nghiêm ngặt được quyết định bởi thành phần bảo đảm sử dụng trong thẩm định): ranh giới TSF của nó sẽ được xác định, đặc tả chức năng của nó được đánh giá để quyết định xem liệu nó mô tả các giao diện tới các dịch vụ an toàn cung cấp bởi TSF, có thể thông tin bổ sung về các TSF (thiết kế, kiến trúc, cấu trúc nội bộ của nó) sẽ được cung cấp, các TSF sẽ được thử nghiệm, các khía cạnh về vòng đời của nó và tài liệu hướng dẫn của nó sẽ được đánh giá, v.v...

Tuy nhiên, việc đánh giá DBMS sẽ không gọi cho bất kỳ bằng chứng liên quan đến sự phụ thuộc DBMS có trên hệ điều hành. Các ST của DBMS hầu như có khả năng phát biểu các giả định về hệ điều hành trong mục giả định của nó và phát biểu các mục tiêu an toàn cho hệ điều hành trong mục Môi trường của nó. Các ST DBMS thậm chí có thể thuyết minh những mục tiêu đó cho môi trường trong điều khoản của SFR cho hệ điều hành. Tuy nhiên, sẽ không có đặc tả cho hệ điều hành phản ánh chi tiết trong các đặc tả chức năng, mô tả kiến trúc, hoặc bằng chứng ADV khác như đối với các DBMS. Sự tin cậy của các thành phần phụ thuộc (ACO_REL) sẽ đáp ứng yêu cầu đó.

Sự tin cậy của các thành phần phụ thuộc (ACO_REL) mô tả các giao diện của TOE phụ thuộc tạo ra các cuộc gọi đến các thành phần cơ sở cho việc cung cấp các dịch vụ. Đây là những giao diện mà các thành phần cơ sở là để đáp ứng. Những mô tả giao diện được cung cấp từ quan điểm của các thành phần phụ thuộc.

Phát triển bằng chứng (ACO_DEV) mô tả các giao diện được cung cấp bởi các thành phần cơ sở, trong đó đáp ứng các yêu cầu dịch vụ thành phần phụ thuộc. Các giao diện này được ánh xạ tới các giao diện thành phần phụ thuộc có liên quan được xác định trong các thông tin tin cậy. (liệu khi các giao diện thành phần cơ sở đã mô tả trình bày tất cả các giao diện thành phần đại diện phụ thuộc, Tính đầy đủ của việc ánh xạ này không xác minh ở đây, nhưng có trong phần sở cứ (ACO_COR)). Ở cấp cao hơn của ACO_DEV các hệ thống con cung cấp các giao diện được mô tả.

Bất kỳ giao diện nào theo yêu cầu của các thành phần phụ thuộc chưa được mô tả cho các thành phần cơ sở được báo cáo trong các lý do cho phần sở cứ (ACO_COR). Sở cứ này cũng báo cáo có các giao diện của các thành phần cơ sở mà trên đó các thành phần phụ thuộc dựa vào được xem xét bên trong đánh giá thành phần cơ sở. Đối với bất kỳ giao diện nào mà không được xem xét trong việc đánh giá thành phần cơ sở, thì sở cứ quy định về tác động của việc sử dụng giao diện trên TSF thành phần cơ sở.

Phụ lục C

(Tham khảo)

Chỉ dẫn tham khảo về các mối phụ thuộc thành phần đảm bảo

Các mối phụ thuộc được dẫn chứng trong các thành phần của mục 9 và 10-16 là những phụ thuộc trực tiếp giữa các thành phần bảo đảm.

Các bảng phụ thuộc đối với các thành phần đảm bảo sau đây chỉ ra các mối phụ thuộc trực tiếp, gián tiếp hay tùy ý của chúng. Mỗi thành phần đó là một các mối phụ thuộc của một số thành phần đảm bảo được phân bổ theo mỗi cột. Còn mỗi thành phần đảm bảo được phân bổ theo hàng ngang. Giá trị mỗi ô trong bảng được đánh dấu "X": chỉ ra các mối phụ thuộc trực tiếp, dấu "-": chỉ sự gián tiếp. Còn nếu trong mỗi ô không có ký tự nào thì các thành phần đó không phụ thuộc.

Bảng C.1 – Bảng phụ thuộc cho lớp ACO: Tổng hợp

	ACO_DEV.1	ACO_DEV.2	ACO_DEV.3	ACO_REL.1	ACO_REL.2	ALC_CMC.1	ALC_CMS.1
ACO_COR.1	X			X		X	-
ACO_CTT.1	X			X			
ACO_CTT.2		X		-	X		
ACO_DEV.1				X			
ACO_DEV.2				X			
ACO_DEV.3					X		
ACO_REL.1							
ACO_REL.2							
ACO_VUL.1	X			-			
ACO_VUL.2		X		-			
ACO_VUL.3			X		-		

Bảng C.2 – Bảng phụ thuộc cho lớp ADV: Phát triển

	ADV_FSP.1	ADV_FSP.2	ADV_FSP.3	ADV_FSP.4	ADV_FSP.5	ADV_FSP.6	ADV_IMP.1	ADV_TDS.1	ADV_TDS.3	ALC_CMC.5	ALC_CMS.1	ALC_DVS.2	ALC_LCD.1	ALC_TAT.1
ADV_ARC.1	X	-						X						
ADV_FSP.1														
ADV_FSP.2		-						X						
ADV_FSP.3		-						X						
ADV_FSP.4		-						X						
ADV_FSP.5		-		-			X	X	-					-
ADV_FSP.6		-		-			X	X	-					-
ADV_IMP.1		-		-			-	-	X					X
ADV_IMP.2		-		-			-	-	X	X	-	-	-	X
ADV_INT.1		-		-			X	-	X					X
ADV_INT.2		-		-			X	-	X					X
ADV_INT.3		-		-			X	-	X					X
ADV_SPM.1		-		X				-						
ADV_TDS.1		X						-						
ADV_TDS.2		-	X					-						
ADV_TDS.3		-		X				-						
ADV_TDS.4		-		-	X		-	-	-					-
ADV_TDS.5		-		-	X		-	-	-					-
ADV_TDS.6		-		-		X	-	-	-					-

Bảng C.3 – Bảng phụ thuộc cho lớp AGD: Tài liệu hướng dẫn

	ADV_FSP.1
AGD_OPE.1	X
AGD_PRE.1	

Bảng C.4 – Bảng phụ thuộc cho lớp ALC: Hỗ trợ vòng đời

	ADV_FSP.2	ADV_FSP.4	ADV_IMP.1	ADV_TDS.1	ADV_TDS.3	ALC_CMS.1	ALC_DVS.1	ALC_DVS.2	ALC_LCD.1	ALC_TAT.1
ALC_CMC.1						X				
ALC_CMC.2						X				
ALC_CMC.3						X	X		X	
ALC_CMC.4						X	X		X	
ALC_CMC.5						X		X	X	
ALC_CMS.1										
ALC_CMS.2										
ALC_CMS.3										
ALC_CMS.4										
ALC_CMS.5										
ALC_DEL.1										
ALC_DVS.1										
ALC_DVS.2										
ALC_FLR.1										
ALC_FLR.2										
ALC_FLR.3										
ALC_LCD.1										
ALC_LCD.2										
ALC_TAT.1	-	-	X	-	-					-
ALC_TAT.2	-	-	X	-	-					-
ALC_TAT.3	-	-	X	-	-					-

Bảng C.5 – Bảng phụ thuộc cho lớp APE: Đánh giá hồ sơ bảo vệ

	APE_ECD.1	APE_INT.1	APE_OBJ.2	APE_REQ.1	APE_SPD.1
APE_CCL.1	X	X		X	
APE_ECD.1					
APE_INT.1					
APE_OBJ.1					
APE_OBJ.2					X
APE_REQ.1	X				
APE_REQ.2	X		X		-
APE_SPD.1					

Bảng C.6 – Bảng phụ thuộc cho lớp ASE: Đánh giá đích an toàn

	ADV_ARC.1	ADV_FSP.1	ADV_FSP.2	ADV_TDS.1	ASE_ECD.1	ASE_INT.1	ASE_OBJ.2	ASE_REQ.1	ASE_SPD.1
ASE_CCL.1					X	X		X	
ASE_ECD.1									
ASE_INT.1									
ASE_OBJ.1									
ASE_OBJ.2									X
ASE_REQ.1					X				
ASE_REQ.2					X		X		-
ASE_SPD.1									
ASE_TSS.1		X			-	X		X	
ASE_TSS.2	X	-	-	-	-	X		X	

Bảng C.7 – Bảng phụ thuộc cho lớp ATE: Kiểm thử

	ADV_ARC.1	ADV_FSP.1	ADV_FSP.2	ADV_FSP.3	ADV_FSP.4	ADV_FSP.5	ADV_IMP.1	ADV_TDS.1	ADV_TDS.2	ADV_TDS.3	ADV_TDS.4	AGD_OPE.1	AGD_PRE.1	ALC_TAT.1	ATE_COV.1	ATE_FUN.1
ATE_COV.1			X					-							-	X
ATE_COV.2			X					-							-	X
ATE_COV.3			X					-							-	X
ATE_DPT.1	X	-	-	-				-	X						-	X
ATE_DPT.2	X	-	-		-			-		X					-	X
ATE_DPT.3	X	-	-		-	-	-	-		-	X			-	-	X
ATE_DPT.4	X	-	-		-	-	X	-		-	X			-	-	X
ATE_FUN.1			-					-							X	-
ATE_FUN.2			-					-							X	-
ATE_IND.1		X										X	X			
ATE_IND.2		-	X					-				X	X		X	X
ATE_IND.3		-	-		X			-				X	X		X	X

- **Bảng C.8** – Bảng phụ thuộc cho lớp AVA: Đánh giá điểm yếu

	ADV_ARC.1	ADV_FSP.1	ADV_FSP.2	ADV_FSP.4	ADV_IMP.1	ADV_TDS.1	ADV_TDS.3	AGD_OPE.1	AGD_PRE.1	ALC_TAT.1
AVA_VAN.1		X						X	X	
AVA_VAN.2	X	X	-			X		X	X	
AVA_VAN.3	X	-	X	-	X	-	X	X	X	-
AVA_VAN.4	X	-	X	-	X	-	X	X	X	-
AVA_VAN.5	X	-	X	-	X	-	X	X	X	-

Phụ lục D

(Tham khảo)

Tham chiếu chéo của PPs và các thành phần đảm bảo

Bảng D.1 mô tả các mối quan hệ giữa PP giữa các họ và các thành phần của lớp APE.

Bảng D.1 – Tóm tắt mức đảm bảo PP

Lớp đảm bảo	Họ đảm bảo	Các thành phần đảm bảo	
		PP đảm bảo mức thấp	PP
Đánh giá hồ sơ bảo vệ	APE_CCL	1	1
	APE_ECD	1	1
	APE_INT	1	1
	APE_OBJ	1	2
	APE_REQ	1	2
	APE_SPD		1

Phụ lục E

(Tham khảo)

Tham chiếu chéo của EALs và các thành phần đảm bảo

Bảng E.1 mô tả mối quan hệ giữa các mức đảm bảo đánh giá với các lớp, họ và thành phần đảm bảo.

Bảng E.1 – Tóm tắt mức đảm bảo đánh giá

Lớp đảm bảo	Họ đảm bảo	Các thành phần đảm bảo theo mức đảm bảo đánh giá (EAL)						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Phát triển	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Tài liệu hướng dẫn	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Hỗ trợ vòng đời	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Đánh giá đích an toàn	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Kiểm thử	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Đánh giá điểm yếu	AVA_VAN	1	2	2	3	4	5	5

Phụ lục F

(Tham khảo)

Chỉ dẫn tham khảo cho các CAP và các thành phần đảm bảo

Bảng F.1 mô tả mối quan hệ giữa các cấp bảo đảm tổng hợp và việc đảm bảo các lớp, họ và các thành phần đảm bảo.

Bảng F.1 – Tóm tắt mức đảm bảo tổng hợp

Lớp đảm bảo	Họ đảm bảo	Các thành phần đảm bảo từ Gói đảm bảo tổng hợp		
		CAP-A	CAP-B	CAP-C
Tổng hợp	ACO_COR	1	1	1
	ACO_CTT	1	2	2
	ACO_DEV	1	2	3
	ACO_REL	1	1	2
	ACO_VUL	1	2	3
Tài liệu hướng dẫn	AGD_OPE	1	1	1
	AGD_PRE	1	1	1
Hỗ trợ vòng đời	ACL_CMC	1	1	1
	ACL_CMS	2	2	2
	ACL_DEL			
	ACL_DVS			
	ACL_FLR			
	ACL_LCD			
	ACL_TAT			
Đánh giá đích an toàn	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD		1	1
	ASE_TSS	1	1	1

Thư mục tài liệu tham khảo

[1] ISO/IEC 15408 – 1 : 2005, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and general model.

[2] ISO/IEC 15408 – 2 : 2005, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security functional requirements.

[3] ISO/IEC 15408 – 3 : 2005, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security assurance requirements.

[4] ISO/IEC 15408 – 1 : 2009, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and general model.

[5] ISO/IEC 15408 – 2 : 2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security functional requirements.

[6] ISO/IEC 15408 – 3 : 2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security assurance requirements.

[7] ISO/IEC 27001: 2005, Information technology — Security techniques — Information security management systems — Requirements

[8] ISO/IEC 27002: 2005, Information technology — Security techniques — Code of practice for information security management

[9] TCVN 27001: 2009, Công nghệ thông tin – Các kỹ thuật an toàn – Các hệ thống quản lý an toàn thông tin — Các yêu cầu