TCVN **T I Ê U C H U Ẩ N Q U Ố C G I A**

TCVN 10607-2:2014
ISO/IEC 15026-2:2011

Xuất bản lần 1

KỸ THUẬT PHẦN MỀM VÀ HỆ THỐNG – ĐẢM BẢO PHẦN MỀM VÀ HỆ THỐNG – PHẦN 2: TRƯỜNG HỢP ĐẢM BẢO

Systems and software engineering –
Systems and software assurance –
Part 2: Assurance case

HÀ NỘI – 2014

Mục lục

Trang

Lời nói đầu....4

1 Phạm vi áp dụng....5

2 Sự phù hợp....5

3 Tài liệu viện dẫn....5

4 Thuật ngữ và định nghĩa....5

5 Sử dụng tiêu chuẩn....6

6 Cấu trúc và nội dung của trường hợp đảm bảo....7

7 Kết quả được yêu cầu của việc sử dụng tiêu chuẩn....12

Thụ mục tài liệu tham khảo....14

Lời nói đầu

TCVN 10607-2:2014 hoàn toàn tương đương với ISO/IEC 15026-2:2011**.**

TCVN 10607-2:2014 do Ban kỹ thuật tiêu chuẩn quốc gia TCVN/JTC 1 *Công nghệ thông tin* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ TCVN 10607 (ISO/IEC 15026) *Kỹ thuật phần mềm và hệ thống* gồm các tiêu chuẩn sau:

- TCVN 10607-1:2014 (ISO/IEC 15026-1:2013) Kỹ thuật phần mềm và hệ thống – Đảm bảo phần mềm và hệ thống – Phần 1: Khái niệm và từ vựng;
- TCVN 10607-2:2014 (ISO/IEC 15026-2:2011) Kỹ thuật phần mềm và hệ thống – Đảm bảo phần mềm và hệ thống – Phần 2: Trường hợp đảm bảo;
- TCVN 10607-3:2014 (ISO/IEC 15026-3:2011) Kỹ thuật phần mềm và hệ thống – Đảm bảo phần mềm và hệ thống – Phần 3: Mức toàn vẹn hệ thống;
- TCVN 10607-4:2014 (ISO/IEC 15026-4:2012) Kỹ thuật phần mềm và hệ thống – Đảm bảo phần mềm và hệ thống – Phần 4: Đảm bảo trong vòng đời.

Kỹ thuật phần mềm và hệ thống – Đảm bảo phần mềm và hệ thống – Phần 2: Trường hợp đảm bảo

Systems and software engineering – Systems and software assurance –

Part 2: Assurance case

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu tối thiểu cho cấu trúc và nội dung của một trường hợp đảm bảo. Trường hợp đảm bảo bao gồm một đòi hỏi mức cao cho đặc tính của một hệ thống hay sản phẩm (hoặc tập các đòi hỏi), lập luận có hệ thống liên quan tới đòi hỏi đó, bằng chứng và các giả định rõ ràng làm cơ sở cho lập luận này. Việc lý luận thông qua nhiều mức đòi hỏi mức thấp, lập luận có cấu trúc này kết nối đòi hỏi mức cao với bằng chứng và các giả định.

Tiêu chuẩn này không nêu ra các yêu cầu về chất lượng nội dung trong một trường hợp đảm bảo. Hơn nữa, tiêu chuẩn này nêu ra các yêu cầu về việc tồn tại các nội dung và cấu trúc của một trường hợp đảm bảo. Trong khi một vài chú thích và các thuật ngữ hơi khác nhau hiện được dùng trong thực tế, tiêu chuẩn này không yêu cầu việc sử dụng một thuật ngữ hoặc một trình diễn địa lý đặc biệt. Tương tự, tiêu chuẩn này không nêu ra các yêu cầu về cách thức triển khai dữ liệu vật lý, mà không có một yêu cầu nào đối với sự dư thừa hay đồng vị.

2 Sự phù hợp

Một trường hợp đảm bảo phù hợp với tiêu chuẩn này nếu đáp ứng các yêu cầu trong Điều 6 và Điều 7.

3 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 10607-1 (ISO/IEC 15026-1), Kỹ thuật phần mềm và hệ thống - Đảm bảo phần mềm và hệ thống - Phần 1: Khái niệm và từ vựng

ISO/IEC 15289, *Systems and software engineering - Content of systems and software life cycle process information products*

4 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa được đưa ra trong TCVN 10607-1.

5 Sử dụng tiêu chuẩn

Nhu cầu và yêu cầu của hệ thống hay sản phẩm liên quan, các tương tác của hệ thống hay sản phẩm với môi trường của nó và các sự kiện, điều kiện thực tế có thể dẫn tới một mục tiêu nhằm đảm bảo rằng hệ thống hay sản phẩm đạt được các đòi hỏi nhất định. Nhằm đáp ứng mục tiêu này, trường hợp đảm bảo hỗ trợ các đòi hỏi này liên quan tới các đặc tính được chọn lựa của hệ thống hay sản phẩm. Trong khi các đặc tính này có thể được chọn lựa vì bất kỳ lý do nào, một lý do phổ biến chọn lọc các đặc tính bởi chúng là rủi ro liên quan và có sự tin tưởng cao là cần thiết trong việc nhận dạng các đặc tính trong một hệ thống hay sản phẩm. Kết quả của việc phát triển một trường hợp đảm bảo là các giá trị và độ không xác định được xây dựng cho mỗi đặc tính của đòi hỏi mức cao. Độ không xác định liên quan tới sự đúng hay sai của các đòi hỏi này là một kết luận thiết yếu của trường hợp đảm bảo.

Bên liên quan có thể đánh giá trường hợp đảm bảo nhằm xác định việc mở rộng của việc đạt được đòi hỏi mức cao theo hệ thống hay sản phẩm và liệu rằng việc đạt được này được thể hiện theo rủi ro hay độ không xác định được phép và bất kỳ hệ quả liên quan nào. Các kết quả liên quan tới đòi hỏi mức cao, sự hỗ trợ đòi hỏi đó theo độ không xác định và hệ quả tạo nên một cơ sở cho việc quản lý rủi ro, việc đạt được cơ sở cho sự tin tưởng thích hợp và hỗ trợ trong việc đưa ra quyết định.

Bên liên quan có thể thường đưa ra quyết định tốt hơn về một hệ thống hay sản phẩm khi độ không xác định của các kết luận liên quan tới các đặc tính này được giảm thiểu. Trong khi một trường hợp đảm bảo là hữu dụng đối với việc đưa ra quyết định theo các bên liên quan có kinh nghiệm (ví dụ: các nhà phát triển và nhà cung cấp dịch vụ), thường là động cơ thúc đẩy chính đối với một trường hợp đảm bảo nhằm hỗ trợ các quyết định quan trọng do bên liên quan không có nền tảng này, ví dụ: những người tham gia trong việc chứng nhận, quy định, thu thập hay kiểm tra hệ thống.

Cách thức trường hợp đảm bảo được sử dụng và lượng nỗ lực dành cho việc xây dựng trường hợp đảm bảo có thể thay đổi rất nhiều do tính chặt chẽ của các đặc tính được chọn lựa, khoảng thời gian áp dụng đòi hỏi, mức độ không xác định, phạm vi của các giả định được tạo ra và rủi ro hay các hệ quả liên quan. Do đó, nội dung cần thiết trong trường hợp đảm bảo thay đổi phụ thuộc vào bên liên quan và ngữ cảnh đánh giá. Ví dụ: dựa trên các yêu cầu hệ thống và đặc tính được quy định bởi đòi hỏi mức cao, một trường hợp đảm bảo có thể được dùng cho mục đích xác minh hay xác thực.

Tiêu chuẩn này nhằm tối ưu hóa việc phát triển và duy trì các trường hợp đảm bảo. Khi phát triển một hệ thống hay sản phẩm mới hoặc việc tạo ra một thay đổi quan trọng, việc phát triển trường hợp đảm bảo cần không tách rời trong các quy trình, kế hoạch, kỹ thuật, hoạt động và các quyết định liên quan đến việc phát triển hệ thống hay sản phẩm đáng quan tâm.

Nhằm cung cấp sự linh hoạt cần thiết và bao trùm nhiều lĩnh vực khi các trường hợp đảm bảo được tối ưu hóa, tiêu chuẩn này dùng một cách tiếp cận chung và đòi hỏi một ánh xạ giữa tiêu chuẩn này và nội dung của bất kỳ sự phù hợp của trường hợp đảm bảo nào. Các yêu cầu cho việc ánh xạ này được nêu trong Điều 7.2.

CHÚ THÍCH 1 Thuật ngữ “độ không xác định” được sử dụng như một thuật ngữ tổng quát, có nghĩa là: “thiếu chắc chắn”. Các cộng đồng khác nhau hạn chế việc áp dụng thuật ngữ này cho việc sử dụng hạn chế, ví dụ: cho các dự đoán sự kiện dự

kiến, cho các phép đo vật lý đã được tạo ra hay không biết, nhưng thuật ngữ trong tiêu chuẩn này áp dụng đối với bất kỳ độ không xác định nào.

CHÚ THÍCH 2 Việc chọn lọc đòi hỏi mức cao và các đặc tính liên quan mà không bị giới hạn trong tiêu chuẩn này nhưng có thể được quy định theo các yêu cầu bên liên quan hoặc được xây dựng bởi bên phê duyệt cho hệ thống hay sản phẩm. Đòi hỏi mức cao có thể là một phần của các yêu cầu và đặc tả chung nhưng có thể xuất phát từ nội bộ hệ thống, liên quan tới điều mà hệ thống phụ thuộc, hoặc chỉ liên quan gián tiếp tới hệ thống đáng quan tâm chính yếu.

CHÚ THÍCH 3 Các giới hạn của trường hợp đảm bảo của một hệ thống hay sản phẩm phải được phản ánh trong hướng dẫn; tài liệu truyền tải, vận hành và bảo trì; đào tạo; vận hành viên và các hỗ trợ người dùng; khả năng thu thập dữ liệu và các dịch vụ liên quan hay đi kèm với hệ thống hay sản phẩm. Hiểu biết về giới hạn này cho phép tránh và nhận diện các vi phạm của giả định tương ứng hoặc điều kiện liên quan tới các đòi hỏi mức cao.

CHÚ THÍCH 4 Văn bản thường đề cập tới một trường hợp đảm bảo hay một đòi hỏi mức cao riêng lẻ, tuy nhiên một hệ thống hay sản phẩm có thể có nhiều trường hợp đảm bảo và một trường hợp đảm bảo có thể có nhiều đòi hỏi mức cao.

6 Cấu trúc và nội dung của một trường hợp đảm bảo

6.1 Tổng quát

Việc mô tả của tiêu chuẩn này về cấu trúc và nội dung của trường hợp đảm bảo, sử dụng thuật ngữ "thành phần" đối với các phần chính của một trường hợp đảm bảo và mô tả các quan hệ giữa các thành phần này. Các yêu cầu tổng quát sau áp dụng cho:

a) Các thành phần của một trường hợp đảm bảo phải rõ ràng, có thể định danh và có thể truy nhập.

CHÚ THÍCH Sự không rõ ràng có thể tránh được bởi việc kết hợp một thành phần với thông tin theo ngữ cảnh của nó, ví dụ: việc định nghĩa của các thuật ngữ được sử dụng, môi trường của hệ thống hay sản phẩm và các định danh thực thể chịu trách nhiệm đối với sự phát triển hay duy trì một thành phần.

b) Mỗi thành phần phải được xác định duy nhất và phải có nguồn gốc xác định, lịch sử chính xác và tính toàn vẹn của nó được đảm bảo.

c) Đối với mỗi thành phần, các nội dung thành phần, thông tin liên quan và các thành phần khác có các mối quan hệ phải được xác định và có thể truy nhập.

CHÚ THÍCH Đối với mỗi thành phần, việc mô tả và các thành phần khác là cần thiết, ví dụ: bằng chứng cho các đòi hỏi và thông tin liên quan như: các kết quả trường hợp thử, được xác định và có thể truy nhập.

d) Một trường hợp đảm bảo phải bao gồm các nội dung phụ trợ được yêu cầu bởi ISO/IEC 15289 cho loại tài liệu này.

CHÚ THÍCH Tiêu chuẩn này không chỉ ra hạn chế về cách thức các nội dung phụ trợ được bao gồm và không có yêu cầu rằng trường hợp đảm bảo là một tài liệu riêng biệt.

6.2 Cấu trúc chung

Năm thành phần chính của một trường hợp đảm bảo là: các đòi hỏi, lập luận, bằng chứng, biện minh và các giả định.

Hình 1 mô tả cấu trúc của các trường hợp đảm bảo. Hình 1 không được viện dẫn.

Đòi hỏi

Một đòi hỏi là một đề xuất được đảm bảo về hệ thống đáng quan tâm. Đòi hỏi có thể đi kèm với thông tin phụ trợ, ví dụ: thời hạn được đề cập trong đề xuất hay độ không xác định của đề xuất.

Biện minh, Lập luận, Bằng chứng và Trường hợp đảm bảo

Biện minh, lập luận, bằng chứng và trường hợp đảm bảo được định nghĩa cùng đệ quy trong hình này.

Đưa ra một đòi hỏi *c*, một biện minh *j* của *c* là một lý do tại sao *c* lại được chọn.

Bình luận: Do vậy, một biện minh được định nghĩa liên quan tới đòi hỏi *c*. Một lập luận (được định nghĩa bên dưới) cũng được định nghĩa liên quan tới một đòi hỏi, nhưng khác biệt với biện minh bởi một biện minh là một lý do cho việc lựa chọn một đòi hỏi, trong khi một lập luận là một lý do tạo sao một đòi hỏi là đúng.

Đưa ra một đòi hỏi *c* và một tập bằng chứng *es*, một lập luận mà đảm bảo *c* dùng *es* được định nghĩa là một lý do tạo sao sự thực của *c* được suy luận từ phần chính của bằng chứng trong tập *es*.

Bằng chứng là cả một thực tế, mốc, đối tượng, một đòi hỏi hay một trường hợp đảm bảo. Một đòi hỏi được gọi là một giả định nếu nó xuất hiện trong một trường hợp đảm bảo như bằng chứng. Phần chính của bằng chứng được định nghĩa dựa trên mẫu bằng chứng, nếu bằng chứng đó là một thực tế, mốc, đối tượng hay một đòi hỏi, phần chính của nó là chính nó; nhưng nếu bằng chứng đó là một trường hợp đảm bảo a_o, phần chính của nó là đòi hỏi của a_o.

Bình luận: Bằng chứng phải được chỉ rõ bên dưới trong Hình 1 rằng: bằng chứng của một trường hợp đảm bảo được dùng bởi một lập luận của trường hợp đảm bảo đó nhằm đảm bảo rằng đòi hỏi của nó được kéo dài.

Bình luận: Một đòi hỏi xuất hiện như một bằng chứng được gọi là một giả định bởi bằng chứng đó là một đề xuất với bất kỳ lý do tại sao lại đúng. Khi một lý do cho sự thật được nêu ra, lý do được mong đợi rằng một trường hợp đảm bảo mà lập luận của nó là lý do đó, được xây dựng và được nêu như bằng chứng thay vì cung cấp chỉ một đòi hỏi như bằng chứng.

Một trường hợp đảm bảo được định nghĩa là một bội số bốn của một đòi hỏi *c*, một biện minh *j* của *c*, một tập bằng chứng *es* và một lập luận *g* mà đảm bảo *c* dùng *es*. Cho $a=(c,j,es,g)$ là một trường hợp đảm bảo; *c* được định nghĩa là đòi hỏi của *a*; tương tự *j* được định nghĩa là biện minh của *a*, *es* là tập bằng chứng của *a*, và *g* là lập luận của *a*.

Bình luận: Định nghĩa các trường hợp đảm bảo dựa trên các lập luận, định nghĩa các lập luận dựa trên bằng chứng và định nghĩa bằng chứng dựa trên các trường hợp đảm bảo. Các định nghĩa này tuy không vòng vo, nhưng cùng đệ quy với các định nghĩa khác.

Bình luận: Đối với người dùng theo định hướng toán học, định nghĩa đệ quy sau của tập các trường hợp đảm bảo có thể giúp đỡ phần nào. Tập trường hợp đảm bảo *A* và tập bằng chứng *E* được định nghĩa bởi các phép toán đệ quy sau:

$$A_0 = C \times \{ j_0 \in J(c_0) \mid c_0 \in C \} \times \omega_f(E) \times \{ g_0 \in G(c_0, es_0) \mid c_0 \in C, es_0 \in \omega_f(E) \}$$

$$A = \{ (c, j, es, g) \in A_0 \mid j \in J(c), g \in G(c, es) \}$$

$$E = F + D + O + C + A$$

trong đó:

$J(c)$	tập tất cả biện minh đối với một đòi hỏi *c*;
C	tập đòi hỏi;
$\omega_f(E)$	tập tất cả tập con hữu hạn của *E* (tập tổng hữu hạn của *E*);
$G(c_0, es_0)$	tập các lập luận đảm bảo một đòi hỏi c_o sử dụng một tập bằng chứng es_o;
F	tập thực tế, *D* là tập thời gian;
O	tập đối tượng;
$M \times N$	sản phẩm trực tiếp của *M* và *N*, với bất kỳ tập *M* và *N* nào; và
$M + N$	nhóm phân biệt (tổng trực tiếp) của *M* và *N* và bất kỳ tập *M* và *N* nào.

Hình 1 - Cấu trúc của trường hợp đảm bảo (tham khảo)

Các đòi hỏi sau áp dụng cho cấu trúc của một trường hợp đảm bảo:

a) Một trường hợp đảm bảo phải có một hay nhiều các đòi hỏi mức cao là mục đích tối thượng của các lập luận của chính trường hợp đảm bảo.

CHÚ THÍCH Nhiều đòi hỏi mức cao tương đương với việc kết nối của chúng.

b) Một lập luận phải được hỗ trợ bởi một hay nhiều đòi hỏi, bằng chứng hay giả định.

CHÚ THÍCH 1 Một lập luận được sử dụng nhằm thể hiện cách thức mà các thành phần làm nền tảng trực tiếp liên quan tới một hay một tập đòi hỏi. Tập các thành phần làm nền tảng với mỗi lập luận bao gồm: một tập bằng chứng, giả định và đòi hỏi mức thấp hơn.

CHÚ THÍCH 2 Khi một lập luận không thể hỗ trợ trực tiếp các lập luận khác, một lập luận mức thấp hơn nên gắn với một đòi hỏi mức thấp hơn mà chuyển sang gắn liền với với lập luận cấp cao hơn.

c) Một đòi hỏi phải được hỗ trợ không chỉ bởi một lập luận, hoặc một hay nhiều đòi hỏi, hoặc giả định.

CHÚ THÍCH Mọi đòi hỏi trong một trường hợp đảm bảo yêu cầu hỗ trợ dưới nhiều mẫu khác nhau. Do đó, một đòi hỏi thì không bao giờ là một thành phần bên dưới của một trường hợp đảm bảo. Một (và chỉ một) lập luận có thể được dùng để hỗ trợ một đòi hỏi. Nói cách khác, một đòi hỏi có thể hỗ trợ (trực tiếp và không thông qua lập luận) bởi một vài tập bằng chứng, giả định hoặc các đòi hỏi mức thấp hơn.

d) Một đòi hỏi, lập luận, bằng chứng hay một giả định phải không hỗ trợ chính nó trực tiếp hay gián tiếp.

CHÚ THÍCH Một đòi hỏi, lập luận, bằng chứng hay giả định đơn lẻ có thể được dùng để hỗ trợ nhiều thành phần.

6.3 Đòi hỏi

6.3.1 Mẫu đòi hỏi

Đòi hỏi phải là một mô tả đúng-sai nhằm chỉ ra các giới hạn giá trị của một đặc tính được định nghĩa rõ ràng - được gọi là đặc tính của đòi hỏi, các giới hạn về độ không xác định về giá trị của đặc tính đáp ứng các giới hạn của đòi hỏi và các giới hạn về điều kiện mà đòi hỏi này được áp dụng.

6.3.2 Nội dung của đòi hỏi

Một đòi hỏi phải có các nội dung được yêu cầu và có thể có nhiều nội dung tùy chọn được chỉ ra trong danh sách sau:

a) Đặc tính của đòi hỏi (yêu cầu).

b) Các giới hạn dựa trên giá trị của đặc tính liên quan tới đòi hỏi (ví dụ: trong dải của nó) (yêu cầu).

c) Các giới hạn dựa trên độ không xác định của giá trị đặc tính đáp ứng giới hạn của nó (yêu cầu).

d) Các giới hạn dựa trên khoảng thời gian áp dụng đòi hỏi (tùy chọn)

e) Độ không xác định của thời hạn liên quan (tùy chọn)

f) Các giới hạn dựa trên điều kiện mà đòi hỏi được áp dụng (yêu cầu)

g) Độ không xác định của điều kiện liên quan (tùy chọn).

h) Nếu một đặc tính trong một đòi hỏi áp dụng cho một vài tập con của các hệ thống, sản phẩm hay các phần tử của chúng, việc xác định bao gồm: các phiên bản hoặc trường hợp liên quan (yêu cầu có điều kiện).

i) Các hệ quả hoặc rủi ro nếu liên quan tới đòi hỏi (yêu cầu có điều kiện).

CHÚ THÍCH 1 Thuật ngữ "giới hạn" được dùng để đáp ứng nhiều tình huống có thể tồn tại. Các giá trị có thể là một hay nhiều giá trị đơn lẻ, một hay nhiều dải giá trị, hoặc đa chiều. Ranh giới của các giới hạn này đôi khi bao gồm việc phân phối khả năng xảy ra, được tăng cường hoặc có các khía cạnh không rõ ràng khác.

CHÚ THÍCH 2 Độ không xác định cũng có thể liên quan tới khoảng thời gian áp dụng và các điều kiện đề ra. Các đòi hỏi cụ thể không cần bao gồm tất cả độ không xác định có thể và chỉ bao gồm chủ yếu một. Trong trường hợp chính xác, độ không xác định có thể là 0.

6.3.3 Phạm vi của điều kiện

Các điều kiện bao gồm bất kỳ thời hạn được quy định nào, được bao trùm bởi việc kết hợp các thành phần của trường hợp đảm bảo hỗ trợ một đòi hỏi phải cùng bao trùm các điều kiện đó, bao gồm bất kỳ giới hạn được quy định nào cho đòi hỏi được áp dụng.

6.3.4 Biện minh của việc chọn lựa đòi hỏi mức cao

Bởi việc chọn lựa một đòi hỏi mức cao và đặc tính của nó là quan trọng để đáp ứng mục tiêu của một trường hợp đảm bảo và thúc đẩy quá trình xây dựng của trường hợp đảm bảo, một đòi hỏi mức cao phải có một biện minh cho lựa chọn của nó.

CHÚ THÍCH Biện minh cho đòi hỏi mức cao là một cách thức để kết nối rủi ro giữa các bên liên quan của hệ thống và cho việc ghi thỏa thuận.

6.4 Lập luận

6.4.1 Đặc tính của lập luận

Một lập luận được dùng để thể hiện cách thức các thành phần làm nền tảng trực tiếp mà liên quan tới một hay một tập đòi hỏi. Một lập luận có thể đặc biệt hữu ích nếu nó dưới dạng một tính toán kỹ thuật hay bằng chứng logic mà không nằm dưới dạng một trường hợp đảm bảo.

Một lập luận có các đặc tính sau:

a) Lập luận phải chỉ ra theo một cách thức mà sử dụng các thành phần trực tiếp bên dưới nó.

b) Lập luận phải đạt được một hay nhiều kết luận liên quan tới mỗi đòi hỏi mà nó hỗ trợ.

c) Lập luận phải xây dựng độ không xác định của mỗi kết luận đạt được.

d) Lập luận phải bao gồm thông tin cần thiết để triển khai hiệu quả theo độ không xác định của nó.

6.4.2 Biện minh về phương pháp luận

Lập luận phải có một biện minh tương ứng cho giá trị hay chất lượng của phương pháp luận của lập luận (ví dụ: tính toán hoặc tranh cãi).

CHÚ THÍCH Nhiều phương pháp luận có thể sử dụng trong các lập luận. Các phương pháp này bao gồm các công cụ sử dụng, thay đổi khả năng áp dụng, nguồn, dẫn tới sự chính xác và độ không xác định và dễ dàng sử dụng. Các lập luận được dùng để hỗ trợ hoặc giảm thiểu các đòi hỏi. Các đòi hỏi, bằng chứng và các giả định làm nền tảng cho một lập luận có các trạng thái không xác định liên quan tới chúng và lập luận có thể ảnh hưởng tới độ không xác định của đòi hỏi sử dụng lập luận.

6.5 Bằng chứng

6.5.1 Nội dung của bằng chứng

Bằng chứng phải bao gồm dữ liệu hay thông tin rõ ràng.

CHÚ THÍCH Có nhiều loại bằng chứng tồn tại. Giữa các báo cáo kinh nghiệm, lịch sử, quan sát, đo đạc, thử nghiệm, các kết quả đánh giá và tuân thủ, việc hiệu chỉnh của lý do thiết kế, phân tích, so sánh các tạo tác, đánh giá, các sai sót và các đảm bảo chất lượng và dữ liệu lĩnh vực khác. Bằng chứng có thể đã tồn tại, được tạo mới hoặc được thu thập, lên kế hoạch dự kiến. Bằng chứng nên hỗ trợ hoặc giảm thiểu các đòi hỏi trong trường hợp đảm bảo. Nội dung bằng chứng có thể khá lớn và phải được tổ chức, định vị và được thể hiện để có thể hiểu được đối với các cá nhân đánh giá, phê duyệt hay trực tiếp sử dụng bằng chứng.

6.5.2 Thông tin liên quan

Bằng chứng phải bao gồm hoặc có trong nó thông tin liên quan:

a) Định nghĩa.

b) Phạm vi áp dụng.

c) Độ không xác định, bao gồm khả năng tin cậy của nguồn thông tin của bằng chứng (ví dụ: độ xác thực, tin cậy và hoàn chỉnh) và độ đo lường chính xác.

CHÚ THÍCH Thông tin có thể chia thành nhiều dạng bao gồm: một hay nhiều trường hợp đảm bảo hoặc thành phần.

6.5.3 Giả định liên quan

Bất kỳ giả định nào liên quan tới bằng chứng phải được bao gồm trong trường hợp đảm bảo.

6.6 Giả định

6.6.1 Mẫu giả định

Một giả định phải chia thành một đòi hỏi và một lý do ứng với nó.

6.6.2 Nội dung của giả định

Giả định có thể có một trong ba loại nguồn gốc. Hai loại vốn đã được kế thừa theo đúng ngữ cảnh và vai trò của chúng trong trường hợp đảm bảo. Có (1) một giả định được ám chỉ bởi các điều kiện được quy định việc hạn chế khả năng áp dụng của (các) đòi hỏi mà nó hỗ trợ và (2) một giả định kế thừa theo một phương pháp lập luận, ví dụ: một mô tả của một thay đổi là một giá trị của một tập các giả định thay đổi cùng nhau bao trùm tất cả khả năng có thể liên quan, chỉ ra mỗi trường hợp theo một chứng cứ của các trường hợp. Có hai loại giả định có độ không xác định là 0.

Loại giả định thứ ba vốn đã không được kế thừa đúng theo ngữ cảnh, nói đúng hơn nó là một đòi hỏi không được đảm bảo hoàn toàn bởi bằng chứng. Loại giả định này phải:

a) Bao gồm một đòi hỏi và một lý do cho nó.

b) Bao gồm một chỉ báo, định danh hoặc mô tả của cơ sở của việc đánh giá độ không xác định liên quan đến sự thật của giả định.

CHÚ THÍCH Đối với kết quả tốt nhất, các giả định này phải có một hay nhiều đặc tính sau: có độ không xác định hoặc rủi ro thấp bởi chúng ít quan trọng hơn trong lập luận; có một tác động yếu trong lập luận; có ảnh hưởng yếu trong các giá trị quan trọng hay hệ quả, hoặc là một vài trong số đó.

6.6.3 Bằng chứng liên quan

Nếu một giả định được đảm bảo hoặc cam kết một phần theo bằng chứng, bằng chứng đó phải tương ứng với nó.

6.7 Biện minh

Một đòi hỏi mức cao có một biện minh cho việc chọn lựa của chính nó (Điều 6.3.4) và một lập luận có một biện minh cho phương pháp lập luận của chính nó (Điều 6.4.2)

6.8 Kết hợp các trường hợp đảm bảo

Nếu một trường hợp đảm bảo kết hợp với một trường hợp đảm bảo khác, một hay nhiều đòi hỏi mức cao của trường hợp đảm bảo được kết hợp phải được đặt trong mỗi cấu trúc của trường hợp đảm bảo gốc theo các đòi hỏi được phép.

CHÚ THÍCH Một phần của một trường hợp đảm bảo có thể cũng là một phần của các trường hợp đảm bảo khác.

7 Kết quả được yêu cầu của việc sử dụng tiêu chuẩn

7.1 Kết quả

Ứng dụng của tiêu chuẩn này có các kết quả sau:

a) Một trường hợp đảm bảo đáp ứng các yêu cầu của Điều 6 phải được cung cấp như một phần tử của hệ thống.

CHÚ THÍCH Là một phần tử của hệ thống, trường hợp đảm bảo chủ yếu được mong đợi nhằm phân tán trong hệ thống và được duy trì khi hệ thống được bảo trì.

b) Một ánh xạ logic đáp ứng các yêu cầu của Điều 7.2 phải được cung cấp như một phần của trường hợp đảm bảo.

c) Các biên bản ghi chép việc đáp ứng trọn vẹn các yêu cầu của tiêu chuẩn này phải được xác định và tham chiếu theo trường hợp đảm bảo.

d) Việc xác định một hay nhiều thực thể khẳng định sự phù hợp phải được cung cấp trong trường hợp đảm bảo.

7.2 Ánh xạ với tiêu chuẩn

Một trường hợp đảm bảo phải:

a) Bao gồm một ánh xạ rõ ràng đối với các thành phần và quan hệ trong Điều 6.

b) Bao trùm tất cả nội dung được quy định trong Điều 6 ngoại trừ việc biện minh bằng văn bản được cung cấp để làm việc khác.

CHÚ THÍCH 1 Bởi ánh xạ này phải đối chiếu từ các trường hợp đảm bảo được phát triển trong một vài đặc tính riêng và tối ưu hóa nhiều ký hiệu, việc ánh xạ này có thể ở bất kỳ dạng rõ ràng nào.

CHÚ THÍCH 2 Việc ánh xạ có thể gán một ý nghĩa và ánh xạ tới một thành phần đã biến mất nếu ánh xạ đó là rõ ràng. Ví dụ: nếu một loại không xác định cụ thể không được quy định rõ ràng thì ánh xạ đó có thể chỉ ra rằng điều này tương đương với việc ánh xạ được quy định và bằng 0.

Thư viện tài liệu tham khảo

[1] Greenwell, William S., John C. Knight, and Jacob J. Pease, "A Taxonomy of Fallacies in System Safety Arguments" 24th International System Safety Conference, Albuquerque, NM, tháng Tám 2006

[2] IEC 60300, *Dependability management* (tất cả các phần)

[3] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems* (tất cả các phần)

[4] IEC 61511*, Functional safety — Safety instrumented systems for the process industry sector* (tất cả các phần)

[5] IEC 61882:2001*, Hazard and operability studies (HAZOP studies) — Application guide*

[6] IEEE Std 1228-1994, *IEEE Standard for Software Safety Plans*

[7] ISO/IEC 12207:2008*, Systems and software engineering — Software life cycle processes*

[8] ISO/IEC 15288:2008*, Systems and software engineering — System life cycle processes*

[9] ISO/IEC 15408*, Information technology — Security techniques — Evaluation criteria for IT security* (tất cả các phần)

[10] ISO/IEC 15504*, Information technology — Process assessment* (tất cả các phần)

[11] ISO/IEC TR 15443*, Information technology — Security techniques — A framework for IT security assurance* (tất cả các phần)

[12] ISO/IEC 16085:2006*, Systems and software engineering — Life cycle processes — Risk management*

[13] ISO/TR 18529:2000*, Ergonomics — Ergonomics of human-system interaction — Human-centred lifecycle process descriptions*

[14] ISO/IEC 19770*, Information technology — Software asset management* (tất cả các phần)

[15] ISO/IEC 21827:2008*, Information technology — Security Engineering — Capability Maturity Model (SSE-CMM)*

[16] ISO/IEC 25010*, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality models*[11]

[17] ISO/IEC 25012:2008*, Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model*

[18] ISO/IEC 25020:2007*, Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Measurement reference model and guide*

[19] ISO/IEC 25030:2007*, Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Quality requirements*

1 Đã được xuất bản.

[20] ISO/IEC 25040, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process*

[21] ISO/IEC 25051:2006, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing*

[22] ISO/IEC 26702:2007, *Systems engineering — Application and management of the systems engineering process*

[23] ISO/IEC 27005:2008, Information technology — Security techniques — Information security risk management

[24] ISO/IEC Directives, Part 2: *Rules for the structure and drafting of International Standards*, xuất bản lần thứ 5, 2004

[25] KELLY , T. "Arguing Safety – A Systematic Approach to Managing Safety Cases", Doctoral Thesis – University of York: Department of Computer Science. tháng Chín 1998

[26] Ministry of Defence. Defence Standard 00-42 Issue 2, Reliability and Maintainability (R&M) Assurance Guidance. Part 3, R&M Case, 6 tháng Sáu 2003

[27] Ministry Of Defence. Defence Standard 00-55 (PART 1)/Issue 4, Requirements for Safety Related Software in Defence Equipment Part 1: Requirements, tháng Mười hai 2004

[28] Ministry of Defence. Defence Standard 00-55 (PART 2)/Issue 2, Requirements for Safety Related Software in Defence Equipment Part 2: Guidance, 21 tháng Tám 1997

[29] Ministry of Defence. Defence Standard 00-56. Safety Management Requirements for Defence Systems. Part 1. Requirements Issue 4, 01 tháng Sáu 2007

[30] Ministry of Defence. Defence Standard 00-56. Safety Management Requirements for Defence Systems. Part 2 : Guidance on Establishing a Means of Complying with Part 1 Issue 4, 01 tháng Sáu 2007

[31] SafSec Project. SafSec Methodology: Guidance Material: Integration of Safety and Security. Có sẵn tại: http://www.altran-praxis.com/safSecStandards.aspx

[32] SafSec Project. SafSec Methodology: Standard: Integration of Safety and Security. Có sẵn tại: http://www.altran-praxis.com/safSecStandards.aspx

[33] Software and Systems Engineering Vocabulary (sevocab). Có sẵn tại: www.computer.org/sevocab/

[34] UK CAA. CAP 670 Air Traffic Services Safety Requirements. UK Civil Aviation Authority Safety Regulation Group, 18 tháng Hai 2010

[35] UK CAA CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases For Aerodrome Operators and Air Traffic Service Providers, 13 tháng Một 2006