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

TCVN 10607-1:2014
ISO/IEC 15026-1:2013

Xuất bản lần 1

KỸ THUẬT PHẦN MỀM VÀ HỆ THỐNG – ĐẢM BẢO PHẦN MỀM VÀ HỆ THỐNG – PHẦN 1: KHÁI NIỆM VÀ TỪ VỰNG

***Systems and software engineering** –*
***Systems and software assurance** –*
Part 1: Concepts and vocabulary

HÀ NỘI – 2014

Mục lục Trang

Lời nói đầu....4

1 Phạm vi áp dụng....5

2 Khả năng áp dụng....5

3 Thuật ngữ và định nghĩa....5

4 Cấu trúc của tiêu chuẩn....11

5 Khái niệm cơ bản....12

6 Sử dụng các phần của bộ TCVN 10607....16

7 Bộ TCVN 10607 và trường hợp đảm bảo....18

8 Bộ TCVN 10607 và mức toàn vẹn....21

9 Bộ TCVN 10607 và vòng đời....22

10 Tổng kết....24

Thư mục tài liệu tham khảo....25

Lời nói đầu

TCVN 10607-1:2014 hoàn toàn tương đương với ISO/IEC 15026-1:2013**.**

TCVN 10607-1:2014 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 1: Khái niệm và từ vựng

Systems and software engineering – Systems and software assurance –

Part 1: Concepts and vocabulary

1 Phạm vi áp dụng

Tiêu chuẩn này xác định các thuật ngữ đảm bảo liên quan và xây dựng một tập có tổ chức của các khái niệm và mối quan hệ nhằm xây dựng một cơ sở cho kiến thức được chia sẻ qua các cộng đồng người dùng cho sự đảm bảo. Tiêu chuẩn này cung cấp cho người dùng thông tin về các tiêu chuẩn khác trong bộ TCVN 10607, bao gồm việc sử dụng kết hợp nhiều tiêu chuẩn. Khái niệm thiết yếu được đưa ra trong bộ tiêu chuẩn này là các *đòi hỏi* trong một *trường hợp đảm bảo* và sự hỗ trợ các đòi hỏi đó thông qua *lập luận* và *bằng chứng*. Các đòi hỏi này được đặt trong ngữ cảnh đảm bảo cho các đặc tính của hệ thống và phần mềm trong quy trình vòng đời của sản phẩm phần mềm hay hệ thống.

Bộ TCVN 10607 không bao gồm việc đảm bảo cho một dịch vụ đang vận hành và quản lý dựa trên cơ sở liên tục.

2 Khả năng áp dụng

2.1 Người dùng

Người dùng bộ TCVN 10607 bao gồm: nhà phát triển, nhà bảo trì các trường hợp đảm bảo và những người muốn phát triển, duy trì, đánh giá hay thâu nhận một hệ thống có các yêu cầu cho các đặc tính cụ thể theo một cách thức chắc chắn hơn về các đặc tính đó và yêu cầu của chúng. Bộ tiêu chuẩn này thường sử dụng các khái niệm và thuật ngữ phù hợp với các tiêu chuẩn: ISO/IEC 12207, ISO/IEC 15288 và bộ ISO/IEC 25000, nhưng người dùng bộ tiêu chuẩn này cần hiểu các khác biệt về các thuật ngữ và định nghĩa mà họ có thể làm quen. Tiêu chuẩn này tập trung làm rõ những khác biệt này.

2.2 Lĩnh vực áp dụng

Mục đích chính của tiêu chuẩn này nhằm hỗ trợ người dùng các tiêu chuẩn khác của bộ TCVN 10607 bằng cách đưa ra ngữ cảnh, các khái niệm và giải thích cho sự đảm bảo, các trường hợp đảm bảo và mức toàn vẹn. Tuy nhiên, việc thực hành đảm bảo là thiết yếu, các chi tiết về cách thức đo, mô tả hay phân tích các đặc tính nào đó không được bao trùm trong tiêu chuẩn này. Đây là nội dung của các tiêu chuẩn viện dẫn được bao gồm trong Thư mục tài liệu tham khảo.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa sau đây.

CHÚ THÍCH Các thuật ngữ và định nghĩa được thống nhất trong bộ TCVN 10607.

3.1 Thuật ngữ liên quan tới đảm bảo và đặc tính

3.1.1

đảm bảo (assurance)

cơ sở cho sự tin tưởng được chứng minh rằng một đòi hỏi đã hoặc sẽ đạt được.

3.1.2

đòi hỏi (claims)

mô tả đúng-sai về các giới hạn dựa trên giá trị của một đặc tính được định nghĩa rõ ràng - được gọi là đặc tính của đòi hỏi - và các giới hạn dựa trên độ không xác định của các giá trị đặc tính nằm trong các giới hạn này, trong khoảng thời gian áp dụng của đòi hỏi theo các điều kiện đề ra.

CHÚ THÍCH 1 Độ không xác định cũng có thể liên kết với khoảng thời gian áp dụng và các điều kiện đề ra.

CHÚ THÍCH 2 Đòi hỏi bao gồm các điều sau:

- Đặc tính của đòi hỏi;
- Các giới hạn dựa trên giá trị của đặc tính liên kết với đòi hỏi đó (ví dụ: trong dải giá trị);
- Các giới hạn dựa trên độ không xác định của giá trị đặc tính đáp ứng các giới hạn của nó;
- Các giới hạn dựa trên khoảng thời gian áp dụng của đòi hỏi;
- Độ không xác định của khoảng thời gian liên quan;
- Các giới hạn dựa trên điều kiện liên kết với đòi hỏi;
- Độ không xác định của điều kiện liên quan.

CHÚ THÍCH 3 Thuật ngữ “giới hạn” được sử dụng thích hợp với nhiều tình huống có thể xảy ra. Các giá trị có thể là một hay nhiều giá trị đơn lẻ, một hay nhiều dải giá trị và có thể là đa chiều. Ranh giới giữa các giới hạn này đôi khi không rõ ràng, ví dụ: các giới hạn có thể gồm các phân bổ khả năng có thể xảy ra và có thể gia tăng.

3.1.3

trường hợp đảm bảo (assurance case)

tạo tác hợp lý, có thể kiểm tra được tạo ra nhằm hỗ trợ luận điểm rằng một (hay một tập) đòi hỏi mức cao được thỏa mãn, bao gồm luận chứng có hệ thống, các bằng chứng cơ bản và giả định rõ ràng nhằm hỗ trợ (các) đòi hỏi này.

CHÚ THÍCH 1 Một trường hợp đảm bảo bao gồm các điều sau đây và mối quan hệ của chúng:

- Một hay nhiều đòi hỏi về các đặc tính;
- Các lập luận để liên kết bằng chứng và bất kỳ giả định nào cho (các) đòi hỏi một cách logic;
- Nội dung bằng chứng và các giả định có thể hỗ trợ các lập luận này cho (các) đòi hỏi;
- Biện minh cho việc chọn lựa đòi hỏi mức cao và phương pháp luận.

3.1.4

khả tín (dependability)

thuật ngữ tập hợp được dùng để mô tả công năng sẵn có và các nhân tố tác động đến nó: công năng đáng tin cậy, công năng khả trì và công năng hỗ trợ duy trì.

CHÚ THÍCH 1 Khả tín chỉ được dùng cho các mô tả tổng quát trong những thuật ngữ bất định lượng.

CHÚ THÍCH 2 ISO/IEC 25010 [99] chú thích rằng: "các đặc điểm của khả tín bao gồm tính có sẵn và sự thừa kế hay các nhân tố tác động bên ngoài tới nó, ví dụ: độ tin cậy, sự chịu đựng khiếm khuyết, khả năng phục hồi, tính toàn vẹn, an ninh, tính khả trì, độ bền và hỗ trợ duy trì". Một số tiêu chuẩn nêu ra tính khả tín (ví dụ: IEC 60300 và IEC 61078 phiên bản 2.0) và nhiều tiêu chuẩn khác nêu ra các chất lượng bên trong nó. IEC 60050-191 nêu ra các định nghĩa liên quan [63].

[Nguồn: IEC 60300-1:2003]

3.2 Thuật ngữ liên quan tới sản phẩm và quy trình

3.2.1

quy trình (process)

tập các hoạt động tương quan và tương tác nhằm chuyển đổi đầu vào thành đầu ra.

[Nguồn: ISO/IEC 15288:2008 và ISO/IEC 12207:2008]

3.2.2

dạng quy trình (process view)

mô tả cách thức mà một mục đích cụ thể và tập các kết quả có thể đạt được bằng cách sử dụng các hoạt động và tác vụ của các quy trình hiện tại.

[Nguồn: Điều D.3, ISO/IEC 15288:2008]

3.2.3

sản phẩm (product)

kết quả của một quy trình.

CHÚ THÍCH 1 Kết quả có thể là các thành phần, hệ thống, phần mềm, dịch vụ, quy tắc, tài liệu hay nhiều hạng mục khác.

CHÚ THÍCH 2 Trong một vài trường hợp, "kết quả" có thể là nhiều kết quả riêng biệt liên quan. Tuy nhiên, các đòi hỏi thường liên quan tới các phiên bản cụ thể của một sản phẩm.

[Nguồn: ISO/IEC 15288:2008 và ISO 9000:2005]

3.2.4

hệ thống (system)

kết hợp của việc tương tác các phần tử được tổ chức nhằm đạt một hay nhiều mục đích đề ra.

CHÚ THÍCH 1 Một hệ thống có thể được coi như một sản phẩm hay các dịch vụ nó mà cung cấp.

CHÚ THÍCH 2 Thực tế, việc giải thích ý nghĩa của hệ thống thường được làm rõ bằng việc sử dụng một danh từ kết hợp, ví dụ: hệ thống không quân. Tương tự, "hệ thống" có thể được thay thế một cách đơn giản bởi một từ đồng nghĩa tùy thuộc ngữ cảnh, ví dụ: không quân, mặc dù nó có thể gây khó hiểu cho một phối cảnh các nguyên lý hệ thống.

[Nguồn: ISO/IEC 15288:2008]

3.2.5

yêu cầu (requirement)

mô tả các chuyển đổi hay biểu thị một nhu cầu, các giới hạn và điều kiện liên quan.

CHÚ THÍCH 1 Các yêu cầu tồn tại ở nhiều mức và việc biểu thị nhu cầu dưới dạng mức cao (ví dụ: yêu cầu thành phần phần mềm)

[Nguồn: ISO/IEC/IEEE 29148:2011]

3.2.6

phần tử hệ thống (system element)

thành phần của một tập các phần tử cấu thành một hệ thống.

CHÚ THÍCH 1 Phần tử hệ thống là một phần riêng biệt của hệ thống, có thể được thi hành nhằm đáp ứng đầy đủ các yêu cầu cụ thể. Phần tử hệ thống có thể là phần cứng, phần mềm, dữ liệu, con người, quy trình (ví dụ: các quy trình cung cấp dịch vụ cho người dùng), thủ tục (ví dụ: các chỉ dẫn cho người vận hành), cơ sở vật chất, vật liệu và các thực thể tự nhiên (ví dụ: nước, quần thể, khoáng sản) hoặc bất kỳ kết hợp nào.

[Nguồn: ISO/IEC 15288:2008]

3.3 Thuật ngữ liên quan tới mức toàn vẹn

3.3.1

mức toàn vẹn (integrity level)

đòi hỏi của một hệ thống, sản phẩm hay phần tử mà bao gồm các giới hạn dựa trên các giá trị của một đặc tính, phạm vi áp dụng và độ không xác định được phép của đòi hỏi về việc đạt được đòi hỏi.

CHÚ THÍCH 1 Mục đích duy trì các giới hạn dựa trên các giá trị của một đặc tính thường liên quan tới các hạng mục liên quan dẫn đến việc duy trì các rủi ro hệ thống trong các giới hạn.

CHÚ THÍCH 2 Phù hợp với TCVN 10607-3..

3.3.2

yêu cầu mức toàn vẹn (integrity level requirements)

tập các yêu cầu cụ thể áp đặt lên các khía cạnh liên quan tới một hệ thống, sản phẩm hay phần tử và các hoạt động liên quan nhằm chỉ ra việc đạt được mức toàn vẹn được gán (đó là đáp ứng đòi hỏi của nó) theo các giới hạn được yêu cầu dựa trên độ không xác định, điều này bao gồm bằng chứng đạt được.

CHÚ THÍCH 1 Khi một mức toàn vẹn được định nghĩa như một đòi hỏi, hai cụm từ: “việc đạt được mức toàn vẹn được gán” và “đáp ứng đòi hỏi của nó” là tương đương.

CHÚ THÍCH 2 Trong Điều 3.3.1 và 3.3.2 của TCVN 10607-3 đề cập tới: “mức toàn vẹn” và “ yêu cầu toàn vẹn” liên quan. Cụm từ thứ hai đã được thay đổi thành: “yêu cầu mức toàn vẹn” nhằm làm rõ ràng hơn và bởi điều này được sử dụng phổ biến trong an toàn.

CHÚ THÍCH 3 Tiêu chuẩn IEEE 1012:2004 định nghĩa “mức toàn vẹn” là “một giá trị thể hiện các đặc tính đặc thù của dự án (ví dụ: độ phức tạp, độ tới hạn, rủi ro, mức an toàn, mức bảo mật, công năng mong đợi và độ tin cậy của phần mềm) xác định tầm quan trọng của phần mềm đối với người dùng”. Do vậy, mức toàn vẹn là một giá trị của đặc tính của phần mềm mục tiêu. Khi một đòi hỏi và một mô tả rằng một đặc tính có giá trị nào đó có thể coi như một đề xuất của một hệ thống hay phần mềm, hai định nghĩa mức toàn vẹn có cùng ý nghĩa.

3.4 Thuật ngữ liên quan tới điều kiện và hệ quả

3.4.1

hệ quả (consequence)

tác động (thay đổi hay không thay đổi), thường liên kết với một sự kiện, điều kiện hoặc hệ thống và thường được cho phép, tạo điều kiện, gây ra, ngăn ngừa, thay đổi hay đóng góp bởi sự kiện, điều kiện hoặc hệ thống.

CHÚ THÍCH 1 Hệ quả có thể mang lại lợi ích, tổn thất hoặc không gì cả.

3.4.2

rủi ro (risk)

kết hợp của khả năng xảy ra một sự kiện và hệ quả của nó.

CHÚ THÍCH 1 Thuật ngữ “rủi ro” thường chỉ được sử dụng khi có khả năng xảy ra các hệ quả tiêu cực ít nhất.

CHÚ THÍCH 2 Trong một vài tình huống, rủi ro phát sinh từ khả năng xảy ra sai lệch từ kết quả hay sự kiện mong đợi.

CHÚ THÍCH 3 Xem TCVN 6844 đối với các vấn đề liên quan tới an toàn.

[Nguồn: ISO/IEC 16085]

3.4.2

hệ quả tiêu cực (adverse consequence)

hệ quả không mong muốn tương ứng với một thiệt hại.

3.4.3

hệ quả mong muốn (hay tích cực) (desireable (or undesireable) consequence)

hệ quả tương ứng với lợi ích, lợi lộc hoặc việc tránh một hệ quả tiêu cực.

3.4.4

sai sót (error)

tình trạng sai của hệ thống.

3.4.5

khiếm khuyết (fault)

nhược điểm trong một hệ thống hay một trình diễn hệ thống mà nếu được thực hiện/kích hoạt có khả năng gây ra một sai sót.

CHÚ THÍCH 1 Khiếm khuyết có thể xuất hiện trong các đặc tả khi chúng không chính xác.

3.4.6

tấn công (attack)

hành động hay sự tương tác có chủ ý gây hại với hệ thống hay môi trường của nó, có khả năng dẫn đến một khuyết điểm, sai sót (và do đó có thể là một lỗi) hay một hệ quả tiêu cực.

3.4.7

vi phạm (violation)

việc làm sai lệch hành vi, hoạt động hay sự kiện từ một đặc tính mong muốn hay đòi hỏi lợi ích của một hệ thống.

CHÚ THÍCH 1 Trong lĩnh vực an toàn, thuật ngữ “vi phạm” được sử dụng nhằm đề cập tới một sự vi phạm cá nhân cố ý của một thủ tục hay quy tắc.

3.4.8

lỗi (failure)

chấm dứt khả năng của một hệ thống nhằm thực hiện một chức năng được yêu cầu hoặc sự không có khả năng/bất lực của nó nhằm thực hiện trong các giới hạn được chỉ rõ trước đó; một sai lệch có thể thấy từ bên ngoài từ đặc tả hệ thống.

3.4.9

lỗi có hệ thống (systematic failure)

lỗi liên quan tới cách thức tất định đối với một nguyên nhân nhất định chỉ có thể bị loại bỏ do một điều chỉnh thiết kế hay quy trình sản xuất, thủ tục vận hành, tài liệu hoặc các nhân tố liên quan.

3.5 Thuật ngữ liên quan tới tổ chức

3.5.1

tổ chức (organization)

một hay một nhóm cá nhân và cơ sở vật chất có một phân bổ các trách nhiệm, thẩm quyền và các quan hệ.

CHÚ THÍCH 1 Một bộ phận cá nhân được tổ chức theo một vài mục đích cụ thể, ví dụ: một câu lạc bộ, hiệp hội, tập đoàn hay cộng đồng là một tổ chức.

CHÚ THÍCH 2 Một bộ phận xác định của tổ chức (thậm chí nhỏ như một cá thể riêng lẻ) hay một nhóm xác định của tổ chức có thể coi là một tổ chức nếu nó có trách nhiệm, quyền hạn và các quan hệ.

[Nguồn: ISO/IEC 15288:2008]

3.5.2

bên phê duyệt (approval authority)

một (hay nhiều) cá nhân và/hoặc một (hay nhiều) tổ chức chịu trách nhiệm cho việc phê duyệt các hoạt động, giả thiết và các khía cạnh khác của hệ thống trong suốt vòng đời của nó.

CHÚ THÍCH 1 Bên phê duyệt có thể bao gồm nhiều thực thể, ví dụ: các cá nhân hay tổ chức. Bên phê duyệt có thể bao gồm các quyền với các mức phê duyệt khác nhau và/hoặc các lĩnh vực quan tâm khác nhau.

CHÚ THÍCH 2 Trong các tình huống hai-bên, bên phê duyệt thường là bên thâu nhận. Trong các tình huống điều tiết, bên phê duyệt có thể là một bên thứ ba, ví dụ: một tổ chức chính phủ hay cơ quan của nó. Trong các tình huống khác, ví dụ: việc đặt mua các sản phẩm thương mại được phát triển bởi một bên thứ ba, sự độc lập của bên phê duyệt có thể là một vấn đề liên quan tới bên thâu nhận.

3.5.3

bên thiết kế (design authority)

cá nhân hay tổ chức chịu trách nhiệm cho việc thiết kế sản phẩm.

3.5.4

bên đảm bảo toàn vẹn (integrity assurance authority)

cá nhân hay tổ chức độc lập chịu trách nhiệm cho việc chứng nhận tuân theo các yêu cầu mức toàn vẹn.

CHÚ THÍCH 1 Phù hợp với TCVN 10607-3, trong đó định nghĩa: “cá nhân hay tổ chức độc lập chịu trách nhiệm cho việc đánh giá sự tuân thủ theo các yêu cầu toàn vẹn”.

4 Cấu trúc của tiêu chuẩn

Điều 5 của tiêu chuẩn này bao gồm các khái niệm cơ bản, ví dụ: sự đảm bảo, bên liên quan, các hệ thống và sản phẩm, độ không xác định và hệ quả. Điều 6 bao gồm các hạng mục về người dùng các tiêu chuẩn: TCVN 10607-2, TCVN 10607-3 và TCVN 10607-4 cần có nhận thức ban đầu. Điều 7, 8 và 9 bao gồm các thuật ngữ, khái niệm và các chủ đề liên quan đặc biệt tới người dùng lần lượt các tiêu chuẩn: TCVN 10607-2, TCVN 10607-3 và TCVN 10607-4, mặc dù người dùng một phần tiêu chuẩn có thể có lợi ích từ một phần thông tin trong các điều đối với các tiêu chuẩn khác. Thư mục tài liệu tham khảo nằm ở phần cuối của tiêu chuẩn này. Các tham chiếu cho các hạng mục được đánh số trong Thư mục tài liệu tham khảo được thể hiện trong các dấu ngoặc vuông.

5 Khái niệm cơ bản

5.1 Giới thiệu

Điều này bao gồm các khái niệm và từ vựng cơ bản cho tất cả các tiêu chuẩn trong bộ TCVN 10607.

5.2 Đảm bảo

Bộ TCVN 10607 sử dụng một định nghĩa cụ thể cho sự đảm bảo làm cơ sở cho sự tin tưởng được chứng minh. Bên liên quan thường cần cơ sở cho sự tin tưởng được chứng minh trước khi phụ thuộc vào một hệ thống, đặc biệt là một hệ thống bao gồm sự phức tạp, sự mới lạ hay công nghệ với một lịch sử các vấn đề (ví dụ: phần mềm). Mức độ phụ thuộc càng lớn thì nhu cầu cho các cơ sở tin tưởng bền vững càng lớn. Các lập luận hợp lệ và bằng chứng thích hợp nhằm xây dựng một lý do hợp lý cho sự tin tưởng được chứng minh theo các đòi hỏi về đặc tính hệ thống liên quan cần được tạo ra. Các đặc tính này có thể bao gồm các khía cạnh: chi phí, hành vi và các hệ quả dự kiến. Trong suốt vòng đời, các cơ sở thích hợp cần tồn tại cho việc biện minh các quyết định liên quan tới việc đảm bảo thiết kế, việc tạo ra một hệ thống thích hợp và có thể phụ thuộc vào hệ thống đó.

Đảm bảo là một thuật ngữ mà việc sử dụng thay đổi trong cộng đồng người sử dụng. Tuy nhiên, tất cả việc sử dụng liên quan tới việc đặt các giới hạn hay giảm độ không xác định như: các phép đo, theo dõi, đánh giá, dự đoán, thông tin, suy luận hay tác động của những điều chưa biết với mục đích tối thượng của việc đạt được và/hoặc thể hiện một đòi hỏi. Sự suy giảm độ không xác định có thể tạo ra một cơ sở hoàn thiện cho sự tin tưởng được chứng minh. Thậm chí nếu việc đánh giá một giá trị đặc tính vẫn không thay đổi, công sức bỏ ra trong việc giảm giá trị của độ không xác định có thể thường được coi là sinh lợi khi dẫn tới việc giảm thiểu độ không xác định nhằm cải thiện cơ sở cho việc đưa ra quyết định.

Đảm bảo có thể liên quan tới (1) hệ thống hay phần mềm được quy định, đáp ứng nhu cầu và kỳ vọng thực tế, hay (2) tạo ra hệ thống được xây dựng và vận hành đáp ứng các đặc tả, hoặc cho cả (1) và (2). Đặc tả có thể là các trình bày của các khía cạnh tĩnh và/hoặc động của hệ thống. Đặc tả thường bao gồm các mô tả khả năng, chức năng, hành vi, cấu trúc, dịch vụ và trách nhiệm bao gồm các khía cạnh thời gian liên quan và tài nguyên liên quan, cũng như các giới hạn dựa trên tần số hay tính nghiêm trọng của sự sai lệch theo sản phẩm và độ không xác định liên quan.

Đặc tả có thể là các quy định và/hoặc giới hạn (ví dụ: đối với và dựa trên các hành vi sản phẩm) cũng như bao gồm các phép đo giá trị và hướng dẫn liên quan tới các thỏa hiệp. Đặc tả thường đặt ra một vài giới hạn khi áp dụng cho môi trường và các điều kiện của nó (ví dụ: nhiệt độ) và có thể là các điều kiện của sản phẩm (ví dụ: tuổi thọ hay lượng sử dụng)

5.3 Bên liên quan

Thông qua hệ thống vòng đời và sản phẩm, các bên liên quan có ảnh hưởng hay bị ảnh hưởng bởi hệ thống và các quy trình vòng đời hệ thống. Bên liên quan có thể có lợi, gánh chịu tổn thất, áp đặt những giới hạn trong hệ thống hoặc có một “cổ phần” trong hệ thống; do đó tạo nên các yêu cầu cho hệ thống. Bên liên quan có thể bao gồm những người không sử dụng mà công năng, các kết quả hoặc

yêu cầu khác có thể bị ảnh hưởng, ví dụ: các thực thể mà phần mềm được thực thi trên cùng các máy tính hay qua kết nối mạng.

Một loại bên liên quan khác nhưng quan trọng là người tấn công, chắc chắn áp đặt những giới hạn hoặc quan tâm tới hệ thống. Tiêu chuẩn này nêu ra người tấn công như một bên liên quan, tuy nhiên trong một số cộng đồng an ninh và cách khác loại trừ người tấn công khỏi việc sử dụng thuật ngữ "bên liên quan".

Bên liên quan tương ứng với các yêu cầu được quan tâm tới không chỉ bao gồm người chủ hay người dùng hệ thống mà còn bao gồm các nhà phát triển và nhà vận hành cần xác định các yêu cầu cho việc phát triển và vận hành hệ thống. Dựa trên các điều kiện và hệ quả, bên liên quan yêu cầu các cơ sở cho sự tin tưởng được chứng minh theo các đặc tả hệ thống cho các yêu cầu được xác định.

5.4 Hệ thống và sản phẩm

Bộ TCVN 10607 sử dụng thuật ngữ "hệ thống" xuyên suốt để nhất quán với ISO/IEC 15288 và ISO/IEC 12207. Người dùng tiêu chuẩn này quen thuộc hơn với việc sử dụng thuật ngữ "sản phẩm" cần chú ý rằng "hệ thống" bao gồm các sản phẩm và dịch vụ là kết quả của các quy trình cũng như phần mềm, hệ thống hoặc các phần tử hay thành phần phần mềm. Trong khi mối quan tâm đối với các hệ thống được cung cấp là thúc đẩy chính (ít nhất là trong Tiêu chuẩn này) bởi các quy trình do con người kiểm soát hay nhân tạo, tiêu chuẩn này có thể được sử dụng nhằm giảm thiểu độ không xác định về sự phụ thuộc của một hệ thống cũng như hiện tượng tự nhiên.

5.5 Đặc tính

Bộ TCVN 10607 liên quan tới sự đảm bảo theo các yêu cầu của một đặc tính hệ thống hay sản phẩm phần mềm. Đặc tính có thể bao gồm một điều kiện, đặc điểm, đặc tính, chất lượng, nét tiêu biểu, phép đo hay một hệ quả. Đặc tính có thể bất biến hay phụ thuộc vào thời gian, tình huống hay lịch sử. Trong bộ tiêu chuẩn này, đặc tính liên quan trực tiếp hay gián tiếp tới một hay nhiều hệ thống và có các yêu cầu liên quan.

Đặc tính có thể có nhiều yêu cầu trạng thái ở quá khứ, hiện tại hoặc tương lai. Tuy nhiên, yêu cầu về trạng thái ở tương lai chính là điều quan trọng nhất của bộ tiêu chuẩn này. Kiến thức này nhằm dự đoán tương lai, nên thường khó khăn hơn và không xác định để đạt được; hơn nữa các hành vi và hệ quả dự kiến của một hệ thống (xem Điều 5.8) thường trở thành các vấn đề chính trong sự đảm bảo.

Nhiều đặc tính với các yêu cầu là chất lượng hệ thống. Nhiều tiêu chuẩn và báo cáo cung cấp các danh sách và định nghĩa chất lượng có thể là chủ đề của sự đảm bảo bao gồm các tiêu chuẩn: ISO/IEC 9126-1, ISO/IEC 25010 và các bộ tiêu chuẩn liên quan: ISO/IEC 2382-12, ISO 9241, ISO/TR 18529 và ISO/TS 25238.

Việc sử dụng thuật ngữ "đặc tính" bắt nguồn từ và nhất quán với việc sử dụng rộng rãi của thuật ngữ "đặc tính" trong ISO/IEC 25010 khi thuật ngữ này được sử dụng các đặc tính mở rộng được kế thừa hoặc không ở bên trong hay bên ngoài và trong việc sử dụng hoặc trong ngữ cảnh.

Các nhà sản xuất và bên liên quan khác có thể ưu tiên các đặc tính, ví dụ: tính hiệu quả, độ tin cậy và thực hiện các nghiên cứu thỏa hiệp giữa họ và các yêu cầu liên quan của họ. Một số công nghệ được

tạo ra nhằm nêu ra các trao đổi này, ví dụ: trong [25], [64], [122], [157] và [40]. Việc quy định rõ một đòi hỏi mức cao cho một đặc tính đôi khi dẫn đến các phân tích bao gồm các nghiên cứu thỏa hiệp.

5.5.1 Đặc tính như hành vi

Đặc tính thường được quy định cụ thể như hành vi. Trong khi các vận hành được thực hiện, các đặc tính của hành vi liên quan có thể được quy định cụ thể một cách hình thức như một kết hợp của:

- Sự hạn chế các trạng thái hệ thống được phép (đôi khi được gọi là “đặc tính an toàn”).
- Các trạng thái hệ thống phải đạt được; tiến trình hay sự hoàn thành được yêu cầu (“đặc tính sống còn”).
- Các liên kết dựa trên các dòng hay tương tác; các yêu cầu cho sự phân tách liên kết.

Các loại đặc tính này có thể nêu ra theo các điều kiện hay liên kết phải chính xác của hệ thống[1]. Thực tế, các đặc tính này là không tầm thường và được mô đun hóa, bao gồm thời gian và (các) trạng thái khởi tạo cũng như các chuyển dịch trạng thái liên quan tới sự tương tác với môi trường của hệ thống hay phần mềm.

Các loại dòng như: khí ga, chất lỏng, giao thông hay thông tin là mối quan tâm có thể có cũng như những liên kết giữa chúng, ví dụ: sự bất giao thoa và sự phân tách nhằm duy trì. Hơn nữa, các liên kết dòng thường thuận tiện hay cần thiết cho các khía cạnh cụ thể của an ninh thông tin [135] bao gồm các cơ chế, chính sách kiểm soát truy cập và các hạn chế về thông tin được trao đổi một cách công khai hay bí mật.

5.6 Độ không xác định và sự tin tưởng

Độ không xác định được dùng trong bộ tiêu chuẩn này như một thuật ngữ bao hàm. Thuật ngữ này bao gồm sự thiếu chắc chắn dù độ không xác định có thể được mô hình hóa theo khả năng có thể xảy ra hay không. Độ không xác định có thể bao gồm các khái niệm không rõ ràng có thể được mô hình hóa mà không có việc sử dụng của khả năng có thể xảy ra. Cộng đồng hiện tại hạn chế áp dụng thuật ngữ này cho các dự đoán về các sự kiện trong tương lai, để các phép đo vật lý sẵn sàng được tạo ra, hoặc cho các điều chưa biết. Trong khi các cách sử dụng bị giới hạn này có thể hữu ích trong các cộng đồng đó, người dùng bộ tiêu chuẩn này bao trùm các cộng đồng khác nhau.

Mức độ tin tưởng có thể là hoặc được đưa ra một cách thích hợp dựa trên một trường hợp đảm bảo cụ thể, có thể thay đổi bởi cá nhân hay tổ chức và tình huống. Độ không xác định về các đòi hỏi của một trường hợp đảm bảo càng thấp thì mức độ tin tưởng hợp lý càng cao. Tuy nhiên, việc chuyển đổi ý nghĩa của độ không xác định thành một mức độ tin tưởng hợp lý theo sự phù hợp cho các ứng dụng hiện tại không phải là không minh bạch hay được hiểu rõ. Vì cơ sở này và nhiều cơ sở khác, các hệ quả đôi khi được đề cập trực tiếp trong trường hợp đảm bảo. Trong khi trường hợp đảm bảo này đóng một khoảng trống logic, độ không xác định không loại bỏ hoạt động đánh giá của người đưa ra quyết định liên quan tới mức độ tin tưởng xứng đáng.

---

[1] Nếu được quy định cụ thể về hình thức, điều này có thể cho phép phân tích tĩnh của sự phù hợp của các thiết kế và mã, việc bổ sung bằng chứng đảm bảo đáng khen ngợi.

[2] Mục đích, ý nghĩa và nhu cầu nhằm phân tách các lỗ hổng từ các điểm yếu khác có thể yếu hoặc không tồn tại. Hơn nữa,

5.7 Điều kiện và sự kiện bắt đầu

Trường hợp đảm bảo cần bao trùm tất cả các điều kiện có thể có một tác động tiêu cực đáng kể trong việc kết luận và độ không xác định của đòi hỏi mức cao. Vô vàn điều kiện và sự kiện tiềm ẩn liên quan có thể khó khăn để xác định trước nhất [2] và việc tìm ra điều gì có thể có một tác động đáng kể có thể khó khăn khi không bao gồm chúng trước nhất, ít nhất trong trường hợp đảm bảo.

Theo lịch sử, một điều kiện nhận được hầu hết sự quan tâm là lỗi hệ thống. Một khối lượng đáng kể các danh sách kiểm tra, thực hành và tài liệu tồn tại đề cập tới lỗi hệ thống (ví dụ: [2], [71] và [14] Chương 18, từ trang 475 tới 524). Trong khi phần lớn công việc này đã được hoàn thành trong các cộng đồng chỉ ra sự an toàn, an ninh hoặc sai sót do con người, lỗi hệ thống có thể dẫn đến việc đạt được một đặc tính hay hệ quả kém hơn cũng như các đặc tính tiêu cực hay tổn thất.

Tính nguy hiểm của các hành vi hệ thống có thể phân biệt bởi các điều kiện của chính môi trường. Các hành vi và điều kiện này thường cần kết hợp trong suốt quá trình phân tích nhằm xây dựng dù các hệ quả tiêu cực có diễn ra hay không. Các điều kiện thực tế của chính môi trường có thể hoặc không được biết đến trong hệ thống dựa trên các cảm biến hay đầu vào hệ thống và việc xử lý chúng.

Nhà thiết kế hệ thống có thể hoặc không được biết rõ tất cả các sự kiện bắt đầu cho một điều kiện trong môi trường, tuy nhiên các điều kiện nguy hiểm cần được giải quyết dù cho không phải tất cả các sự kiện bắt đầu đều được biết đến hoặc có thể nhận ra.

5.8 Hệ quả

Bên ngoài hệ thống, nhiều cơ sở dựa trên các điều kiện có thể dẫn tới các hệ quả tiêu cực, sự kiện bắt đầu hoặc điều kiện tiên quyết của chúng. Trong hệ thống, cơ sở dựa trên các điều kiện mà có thể dẫn tới các hành vi hệ thống nguy hại, sự kiện bắt đầu hay các điều kiện tiên quyết cho các điều kiện này.

Trên thực tế, các đòi hỏi có thể mở rộng ra ngoài các ranh giới của hệ thống hoặc các hành vi. Đặc biệt, các đòi hỏi có thể đặt ra các giới hạn về hệ quả của hành vi của một hệ thống và/hoặc các sự kiện, hoạt động, điều kiện của hệ thống liên quan - đặc biệt là theo các giá trị hệ quả. Hệ quả đó có thể là:

Một hệ quả là mong đợi hoặc không mong đợi theo tầm nhìn, quan điểm hay sự quan tâm của một bên liên quan. Một hệ quả có thể xảy ra bất kỳ đâu trong vòng đời hệ thống.

Trong các hệ thống kỹ thuật-xã hội phức tạp, các giải thích về tai nạn hay vi phạm sự đòi hỏi không thể bị giới hạn cho các lỗi “thành phần”. Hệ quả tiêu cực có thể là kết quả của sự biến đổi hành vi thông thường và những tương tác không chủ tâm hay không dự kiến trước.[57][54] Không đề cập tới cách thức chúng phát sinh, các điều kiện nguy hiểm và hệ quả tiêu cực là đối tượng giảm thiểu.

Người tấn công có thể có các khả năng, tài nguyên, động lực và mục đích cho phép họ khởi tạo và thực hiện các nỗ lực nguy hại nhằm vi phạm một đòi hỏi. Người vi phạm sử dụng khả năng của họ

nhằm tận dụng ưu thế của các cơ hội được hệ thống và/hoặc được môi trường cung cấp được gọi là các lỗ hổng, ví dụ: "điểm yếu có thể bị khai thác hoặc được kích hoạt bởi một nguồn đe dọa" [150] [2])

Một điểm đôi khi bị hiểu lầm là tính nguy hiểm và sự phá hoại là những quan tâm ngay cả khi không có đặc tính hệ thống an ninh liên quan nào được bao gồm. Nhà phát triển nguy hại có thể có một tác động dựa trên việc đạt được thành công của hầu hết các đặc tính.

Nhiều tiêu chuẩn hay báo cáo đề cập tới các hệ quả liên quan tới các hệ thống trong một lĩnh vực cụ thể. Ví dụ bao gồm các tiêu chuẩn: ISO 14620 [79] , ISO 19706 [81] và ISO/TS 25238 [121]. Các tiêu chuẩn quản lý rủi ro cũng nêu ra các hệ quả, ví dụ các tiêu chuẩn: ISO/IEC 16085 [91] và ISO 31000.

6 Sử dụng các phần của bộ TCVN 10607

6.1 Giới thiệu

Bộ tiêu chuẩn này hay các tiêu chuẩn của nó có thể được sử dụng độc lập hoặc với các tiêu chuẩn hay hướng dẫn khác. Tiêu chuẩn này có thể được ánh xạ tới hầu hết các tiêu chuẩn vòng đời và có thể sử dụng bất kỳ tập chất lượng hay đặc tính được xác định rõ nào.

6.2 Hướng dẫn sử dụng ban đầu

Các đặc tính và/hoặc đòi hỏi được bao trùm khi sử dụng bộ tiêu chuẩn này là hoàn toàn phụ thuộc vào người dùng tiêu chuẩn, đáp ứng các nhu cầu và yêu cầu hệ thống của bên liên quan. Bất kỳ đặc tính hay đòi hỏi nào có thể được chọn lọc cho một trường hợp đảm bảo, không kể tới tầm quan trọng hay các rủi ro liên quan; tuy nhiên tiêu chuẩn này được thiết kế chủ yếu cho các đặc tính đó mà một hay nhiều bên liên quan chủ yếu cho là quan trọng. TCVN 10607-4 sử dụng thuật ngữ "đặc tính quan trọng" cho các ưu tiên và yêu cầu của bên liên quan.

Trong khi TCVN 10607-3 thường tương thích ngược với ISO/IEC 15026:1998, việc chuyển đổi thành TCVN 10607-3 yêu cầu xử lý một vài khác biệt. TCVN 10607-3 đưa ra các tùy chọn quyết định và kỹ thuật mới, do tiêu chuẩn này không chỉ được coi như một quan điểm độc lập mà còn bao gồm sự liên quan các mức toàn vẹn cho một trường hợp đảm bảo. TCVN 10607-3 tập trung nhiều vào chính hệ thống và các mức toàn vẹn hơn là sự phân tích rủi ro bên ngoài và sự tạo ra các mức toàn vẹn. Điều 8 thảo luận về các mức toàn vẹn.

6.3 Mối quan hệ giữa các phần của bộ TCVN 10607

Các phần của bộ TCVN 10607:

- TCVN 10607-1 *Phần 1: Khái niệm và từ vựng*, giải thích các khái niệm và thuật ngữ như một cơ sở cho tất cả các phần của bộ tiêu chuẩn này.
- TCVN 10607-2 *Phần 2: Trường hợp đảm bảo*, bao gồm các yêu cầu về nội dung và cấu trúc của trường hợp đảm bảo.

[2] Mục đích, ý nghĩa và nhu cầu nhằm phân tách các lỗ hổng từ các điểm yếu khác có thể yếu hoặc không tồn tại. Hơn nữa, một câu hỏi luôn tồn tại theo các ngữ cảnh hiện tại hay dự kiến liên quan tới: "có thể được khai thác hay kích hoạt".

- TCVN 10607-3 *Phần 3: Mức toàn vẹn hệ thống*, liên quan tới các mức toàn vẹn của trường hợp đảm bảo và bao gồm các yêu cầu cho việc sử dụng các yêu cầu đó có và không có một trường hợp đảm bảo (soát xét ISO/IEC 15026:1998).
- TCVN 10607-4 *Phần 4: Đảm bảo trong vòng đời*, đưa ra hướng dẫn và các khuyến nghị đảm bảo liên quan cho các hoạt động cụ thể trong suốt các quy trình vòng đời hệ thống và phần mềm.

Trong khi các tiêu chuẩn: TCVN 10607-2, TCVN 10607-3 và TCVN 10607-4 nêu ra một phân tách các chủ đề đảm bảo và có thể được dùng riêng rẽ, các tiêu chuẩn này có thể được dùng kết hợp do chúng tạo ra một tập liên quan. Tiêu chuẩn này đưa ra nền tảng, các khái niệm và từ vựng được áp dụng cho ba tiêu chuẩn còn lại và các giới thiệu cụ thể nhằm bao trùm các tiêu chuẩn: TCVN 10607-2, TCVN 10607-3 và TCVN 10607-4.

Trường hợp đảm bảo liên quan tới một mở rộng lớn hay nhỏ hơn trong tất cả các phần của bộ tiêu chuẩn này, mặc dù TCVN 10607-4 thảo luận việc đạt được đòi hỏi và thể hiện việc đạt được đòi hỏi dù có hay không việc "thể hiện" đó được đặt trong một tạo tác được gọi cụ thể là một "trường hợp đảm bảo".

TCVN 10607-2 tập trung vào nội dung và cấu trúc của trường hợp đảm bảo. TCVN 10607-3 liên quan tới các mức toàn vẹn và trường hợp đảm bảo bằng việc mô tả cách thức các mức toàn vẹn và trường hợp đảm bảo có thể cùng làm việc, đặc biệt trong định nghĩa các đặc tả mức toàn vẹn hoặc bằng việc sử dụng các mức toàn vẹn trong một phần của trường hợp đảm bảo. Mối quan hệ này được quản lý theo mức độ rủi ro và các phụ thuộc trong hệ thống.

Nếu các rủi ro hay cách xử lý rủi ro không được biết rõ, hoặc nếu cấu trúc phụ thuộc của toàn bộ hệ thống, hoặc việc lựa chọn các đòi hỏi phù hợp không rõ ràng thì việc sử dụng một trường hợp đảm bảo là lựa chọn tốt hơn việc sử dụng các mức toàn vẹn. Cụ thể trong trường hợp này, khi đối mặt với các loại rủi ro mới hay sử dụng một loại xử lý rủi ro mới. Trong các tình huống này, việc biện minh chọn lựa đòi hỏi mức cao cho trường hợp đảm bảo là quan trọng.

Khi các rủi ro và việc xử lý rủi ro được biết rõ, tuy nhiên các nhà phát triển không cần biện minh việc chọn đòi hỏi mức cao và chỉ cần chọn lọc các đòi hỏi thích hợp cho ngữ cảnh của một tập đã biết của chúng - một mức toàn vẹn từ một tập các mức toàn vẹn. Trong các tình huống này, các lập lập chung được tạo ra bởi người định nghĩa mức toàn vẹn, đưa ra biện minh nhằm đáp ứng các yêu cầu mức toàn vẹn được thể hiện đầy đủ sự đáp ứng mức toàn vẹn. Một biện minh (ví dụ: trường hợp đảm bảo tổng quát) thường được tạo một lần bởi một tổ chức riêng và được dùng bởi nhiều dự án.

TCVN 10607-4 bao trùm hướng dẫn và các khuyến nghị đảm bảo liên quan cho các hoạt động thông qua các quy trình vòng đời, bao gồm các hoạt động nhằm mở rộng qua các quy trình vòng đời đó, liên quan trực tiếp tới một trường hợp đảm bảo, ví dụ: việc lập kế hoạch dự án cho các xem xét đảm bảo liên quan.

6.4 Thẩm quyền

Các tiêu chuẩn của bộ TCVN 10607 bao gồm "thẩm quyền" được định nghĩa trong Điều 3, Thuật ngữ và định nghĩa. Ví dụ: TCVN 10607-3 bao gồm việc đạt được các thỏa thuận giữa bên thiết kế và bên

đảm bảo toàn vẹn. Hơn nữa, một hệ thống mới cần các bên phê duyệt của nhà thâu nhận nhằm đổi lấy việc phân tích quy trình tạo ra các trường hợp đảm bảo với bên thiết kế và bên đảm bảo toàn vẹn của nhà cung cấp.

Tuy nhiên, “bên phê duyệt” cho trường hợp đảm bảo không cần thiết đánh giá sự phù hợp một phần của bộ tiêu chuẩn này. Để mở rộng các đòi hỏi khả dụng của sự phù hợp với các phần được đánh giá theo các khía cạnh minh bạch hơn và khó bị nghi ngờ hơn là chất lượng của các tạo tác và quyết định được đánh giá theo ngữ cảnh của hệ thống hay dự án. Thực tế, các hợp đồng có thể kêu gọi rõ nhà thâu nhận là bên phê duyệt hay người phê duyệt sự phù hợp cho các phần của bộ tiêu chuẩn này.

7 Bộ TCVN 10607 và trường hợp đảm bảo

7.1 Giới thiệu

TCVN 10607-2 bao gồm cấu trúc và nội dung của một trường hợp đảm bảo. Tiêu chuẩn này mô tả năm thành phần cơ bản của một trường hợp đảm bảo: các đòi hỏi, lập luận, bằng chứng, biện minh và các giả định. Mục đích của một trường hợp đảm bảo nhằm tăng cường các kết nối đảm bảo bằng cách thông báo việc đưa ra quyết định của nhà cung cấp và hỗ trợ cơ sở cho sự tin tưởng của nhà cung cấp cần thiết. Việc sử dụng phổ biến của một trường hợp đảm bảo nhằm cung cấp sự đảm bảo các đặc tính hệ thống với các bên, không chỉ liên quan chặt chẽ trong các quy trình phát triển kỹ thuật của hệ thống. Các bên có thể liên quan trong việc chứng nhận hay điều chỉnh, thu thập hay kiểm tra hệ thống. Thông thường, một trường hợp đảm bảo nêu ra các lý do mong đợi và xác nhận sự sản xuất thành công của hệ thống, bao gồm các khả năng xảy ra và rủi ro được xác định như các khó khăn hay chướng ngại nhằm phát triển và duy trì hệ thống đó.

Không giống các chứng cứ logic của việc giảm thiểu các đòi hỏi theo bằng chứng, bao trùm sự thật cần thiết hoặc các khía cạnh sự thật Platonix, các trường hợp đảm bảo giải quyết các khía cạnh biện chứng của hệ thống khi sự thật luôn luôn là tương đối hay thậm chí chủ quan. Nói cách khác, các chứng cứ logic được mô tả theo một thuyết logic cố định, nhưng các trường hợp đảm bảo có thể bị bác bỏ trên cơ sở nhằm làm cơ sở cho thuyết logic là không phù hợp. Nhu cầu cho trường hợp đảm bảo phát sinh khi một trường hợp đảm bảo nhận ra các đặc tính hệ thống thực tế không thể được chuẩn hóa hoàn toàn theo một lý thuyết logic, nhưng luôn luôn có điều gì đó không được bao trùm bởi bất kỳ chuẩn hóa logic nào.

CHÚ THÍCH Khi đòi hỏi mức cao về sự an toàn, an ninh, khả tín hoặc RAM (độ tin cậy, tính sẵn có và khả trì), các trường hợp đảm bảo tương ứng với các đòi hỏi đó được gọi là: các trường hợp an toàn, trường hợp an ninh, trường hợp khả tín hoặc các trường hợp RAM một cách tương ứng. Xem [139], [142], [143], [146], [154], [155], [168], [74], [22], [23], và [24] trong Thư mục tài liệu tham khảo.

Được xem xét như một tạo tác, một trường hợp đảm bảo có các khía cạnh chất lượng liên quan, ví dụ: bản chất nội dung, nguyên mẫu hay cấu trúc của nó (ví dụ: phương pháp luận hoặc mô đun hóa), các vấn đề ngữ nghĩa, ví dụ: sự hoàn thiện, khởi tạo và duy trì bao gồm hỗ trợ công cụ, khả năng sử dụng và trình diễn, sự toàn vẹn, khả dụng, khả năng hiểu biết và có các kết luận được nêu ra với các mức rõ ràng của độ không xác định. Một tiêu đề [164] bao trùm một danh sách đáng kể các đặc tính chất lượng

liên quan cho các trường hợp đảm bảo. Các khía cạnh chất lượng liên quan của một trường hợp đảm bảo không được bao trùm trong TCVN 10607-2 hay bất kỳ phần nào của bộ tiêu chuẩn này.

Bất kỳ sự điều chỉnh đáng kể nào trong hệ thống, thay đổi trong môi trường hay theo các đòi hỏi mức cao của trường hợp đảm bảo cần ghi chép bắt buộc những thay đổi với trường hợp đảm bảo. Do vậy, một trường hợp đảm bảo thường bao gồm sự mở rộng từng bước các bằng chứng được xây dựng trong suốt quá trình phát triển và các hoạt động vòng đời sau này nhằm đáp ứng như được yêu cầu với tất cả thay đổi liên quan [[139] trang 5]

CHÚ THÍCH (Các) đòi hỏi của một trường hợp đảm bảo theo các giá trị đặc tính có thể bao gồm toàn bộ tập yêu cầu của hệ thống cho một đặc tính đáng quan tâm. Một ví dụ về một đòi hỏi mức cao, bao gồm (1) các giới hạn cần thiết theo hệ quả (2) tính năng và các đặc tính của chính hệ thống (ví dụ: tính năng này không được bỏ qua). Chất lượng được định nghĩa trong bộ ISO/IEC 25000 bao gồm chất lượng liên quan tới các tính năng và giới hạn. Tiêu chuẩn Chung phiên bản 3.1 Sửa đổi 2 [30] cũng quan tâm đến cả hai điều này.

7.2 Biện minh về phương pháp luận

Một lập luận có một biện minh tương ứng cho tính hợp lý hay giá trị của chính phương pháp luận. Phương pháp luận có thể là một nguồn bổ sung của độ không xác định.

Một loạt cơ sở cho việc lập luận và phân tích trong trường hợp đảm bảo có thể được sử dụng và những thay đổi này theo khả năng áp dụng, nguồn lực, dẫn tới tính chính xác, độ không xác định và việc sử dụng dễ dàng. Người dùng và các cách tiếp cận với cơ sở khác nhau giữa các cộng đồng có các động lực, tư duy khác nhau và thường có nhiều phương pháp luận.

Ví dụ của phương pháp luận bao gồm:

- Định lượng:
  - Tất định (ví dụ: các chứng minh hình thức).
  - Các hệ thống hình thức luận phi tất định:
    - Xác suất,
    - Lý thuyết trò chơi (ví dụ: minimax), hoặc
    - Các hệ thống suy luận hình thức khác dựa trên độ không xác định (ví dụ: các tập mờ).
- Định tính (ví dụ: đánh giá hiệu năng công việc của nhân viên, phán quyết tòa án, các mô tả định tính về tính nhân quả của sự kiện)

Các sản phẩm và tình huống phức tạp - và bất kỳ điều gì liên quan tới con người – nằm ngoài trạng thái kỹ thuật hiện tại nhằm tạo ra “một cách định lượng” các dự đoán chính xác và tỉ mỉ. Việc đánh giá chủ quan được sử dụng khi không có những phương pháp và kỹ thuật vừa tầm, phù hợp và khách quan hơn hoặc những điều cần bổ trợ hay đánh giá kết quả của những phương pháp kỹ thuật đó. Việc hỗ trợ các kỹ thuật định lượng theo đánh giá và phê bình của chuyên gia được sử dụng rộng rãi và được chấp thuận phổ biến. Với các mẫu lập luận khác, đánh giá chủ quan theo dạng thức của một đòi hỏi và hỗ trợ của nó. Trong khi đôi lúc cần thiết hay hiệu quả, việc sử dụng các đánh giá chủ quan

trong trường hợp đảm bảo có thể dẫn tới độ không xác định bổ sung, nên (chỉ với các giả định) việc xử lý thường càng ít nghiêm trọng thì càng tốt.

Các khung của sự xuất hiện các sự kiện "tự nhiên" và phổ biến, hành vi con người không nguy hại thường được mô tả theo khả năng xảy ra. Tuy nhiên, khả năng cho các hoạt động thông minh, nguy hại mà khả năng có thể không được xác định hoặc không biết đến, đặc biệt là một điều cần quan tâm nếu đối thủ thông minh, nguy hiểm cố tình vi phạm bất kỳ đánh giá khả năng xảy ra nào mà một cá nhân có thể tạo ra liên quan tới hành của chính họ, ví dụ: nhằm tạo ra sự bất ngờ. Nét khác biệt này là trung tâm của sự khác biệt trong suy luận giữa an toàn và an ninh.

7.3 Cách thức thu thập và quản lý bằng chứng

Đối với bất kỳ đặc tính nào, có nhiều cách thức thu thập bằng chứng tồn tại. Đó là lịch sử, kinh nghiệm, khả năng quan sát, các phép đo, thử nghiệm, đánh giá và sự tuân thủ kết quả, các phân tích, tác động và suy luận của con người. Bằng chứng cần đạt được những mục tiêu đưa ra trong lập luận đảm bảo (Điều 9.1, Mod DefStan 00-42 Phần 3 [139])

Bằng chứng có thể trở nên khá lớn, cần được tổ chức và quản lý bởi một số khung cung cấp sự cố định và khả năng truy xuất bằng chứng nhằm cung cấp cho người dùng sự tin tưởng về nguồn gốc, nội dung và tính hợp lệ. Hướng dẫn [150] nêu ra rằng:

- Bằng chứng phải được nêu ra đơn nhất để các lập luận có thể tham chiếu đơn nhất theo bằng chứng.
- Bằng chứng phải được xác thực và kiểm tra.
- Bằng chứng phải được bảo vệ và kiểm soát bởi việc quản lý cấu hình.
- Bằng chứng cần đi kèm với siêu dữ liệu cần thiết để sử dụng một cách chính xác trong trường hợp đảm bảo.

Điều cuối đơn giản là sự tái diễn việc kiểm tra bằng chứng đạt được, liên quan tới trường hợp đảm bảo.

7.4 Chứng nhận và công nhận

Mỗi khía cạnh với các hệ quả tiềm ẩn đáng kể cho việc đáp ứng đòi hỏi mức cao hoặc cho sự tin tưởng các bên liên quan có một vị trí tiềm ẩn trong một bằng chứng của trường hợp đảm bảo toàn diện. Bằng chứng đó không chỉ đưa ra niềm tin nhất quán với các bên liên quan mà còn bao gồm đầy đủ thông tin được sử dụng bởi người chứng nhận và người công nhận.

Công nghiệp hàng không và năng lượng nguyên tử có lịch sử lâu đời về các tiêu chuẩn, chứng nhận, và Hội đồng an ninh ISO/IEC JTC1/SC 27 đã làm việc theo chủ đề đảm bảo trong nhiều năm qua. Các ví dụ an ninh bao gồm các Tiêu chuẩn chung: FIPS 140 cho Mã hóa, TCVN ISO/IEC 27002 *Công nghệ thông tin - Mã thực thi cho quản lý an ninh thông tin* kết hợp với TCVN ISO/IEC 27001 (theo tiêu chuẩn Anh Quốc BS 7799-2:2002) tạo nên một cơ sở cho việc chứng nhận Hệ thống Quản lý An ninh Thông tin (ISMS) của một hệ thống vận hành. Bộ Quốc phòng và Cục Hàng không Nội địa Anh Quốc cũng đưa ra các tiêu chuẩn đáng quan tâm bao gồm các tiêu chuẩn dựa trên trường hợp đảm bảo cho độ tin

cậy, tính khả trì và an toàn - ví dụ: [139], [142], [143], [22] và [23]. Nhiều tiêu chuẩn đã được lên liệt kê Thư mục tài liệu tham khảo.

Cộng đồng an toàn (ví dụ: hàng không thương mại) có chứng nhận sử dụng (đơn vị được chỉ định hay cấp giấy phép) của cá nhân quan trọng như một phần của các cách tiếp cập. Nhiều chứng nhận an ninh máy tính và an toàn tồn tại từ những chứng nhận theo định hướng quản lý tới chứng nhận theo định hướng kỹ thuật về những sản phẩm cụ thể, ví dụ: các chứng nhận từ Ủy ban Chứng nhận An ninh Hệ thống Thông tin Quốc tế (ISC) và viện SANS.

8 Bộ TCVN 10607 và mức toàn vẹn

8.1 Giới thiệu

Các mức toàn vẹn phù hợp cho việc sử dụng các mức rủi ro nhất định hoặc nhằm hỗ trợ một trường hợp đảm bảo và áp đặt tiêu chí đặc biệt theo dự án, bằng chứng được thu thập và hệ thống. Một mức toàn vẹn có thể xem như là một trình diễn mức độ tin tưởng được sử dụng nhằm đạt được thỏa thuận giữa các bên liên quan của một hệ thống theo các rủi ro liên quan đến hệ thống đó.

TCVN 10607-3 xây dựng một khung mức toàn vẹn trước nhất. Phần còn lại của tiêu chuẩn này bao gồm việc định nghĩa, sử dụng các mức toàn vẹn, xác định các mức toàn vẹn sản phẩm hay hệ thống sử dụng các phân tích rủi ro, việc gán các mức toàn vẹn phần tử hệ thống, đáp ứng các yêu cầu mức toàn vẹn sử dụng bằng chứng, các thỏa thuận và phê duyệt liên quan tới các thẩm quyền (xem Điều 6.4)

Các yêu cầu mức toàn vẹn phản ánh điều được yêu cầu để đạt được và thể hiện rằng hệ thống hay phần tử hệ thống (hoặc đã có hoặc sẽ có) các đặc tính được đòi hỏi theo mức toàn vẹn của chính nó. Các trạng thái mức toàn vẹn của một hệ thống phải tương ứng theo các thuật ngữ đặc tính trong toàn bộ hệ thống. Do vậy, việc thể hiện các đặc tính có một vai trò cơ bản trong việc thể hiện sự đáp ứng các đòi hỏi lớn hơn của hệ thống và môi trường của chúng, bao gồm các hệ quả mong muốn và không mong muốn. Nếu các đòi hỏi lớn hơn không được tạo ra thì việc đạt được và thể hiện các mức toàn vẹn phần tử hệ thống cung cấp một phần cơ bản của sự thể hiện đòi hỏi mức cao liên quan tới chính hệ thống.

Thực tế, các mức toàn vẹn thường được thảo luận trong các thuật ngữ nhằm nhấn mạnh bằng chứng cần thiết nhằm đáp ứng các yêu cầu mức toàn vẹn, từ đó cung cấp bằng chứng cho các lập luận hỗ trợ các đòi hỏi liên quan tới các đặc tính của chính hệ thống. Tuy nhiên, chất lượng của việc biện minh các lập luận cho việc đáp ứng các yêu cầu mức toàn vẹn như việc thể hiện việc đạt được mức toàn vẹn liên quan của nó cũng quan trọng bởi ảnh hưởng của chất lượng theo độ không xác định. Độ không xác định liên quan tới lập luận, bằng chứng và giả định là một phần của việc xây dựng các yêu cầu mức toàn vẹn.

CHÚ THÍCH Mức toàn vẹn và tiêu chuẩn tối ưu hóa các mức toàn vẹn có một lịch sử quan trọng, đặc biệt là trong sự an toàn. Mức toàn vẹn trong tiêu chuẩn liên quan đến sự an toàn được định nghĩa trong các tập đa mức, nêu ra các thay đổi mức độ chặt chẽ và/hoặc độ không xác định của việc đạt được mức cao hơn nhằm tạo ra tính chặt chẽ cao hơn và độ không xác

định thấp hơn. Ví dụ của tiêu chuẩn an toàn là IEC 61508 *Functional safety of electricl/electronic/programmable electronic safety-related systems* [70] Tương tự, nhiều lược đồ tương đương được dùng với các nhãn khác nhau, ví dụ: "lớp phù hợp".

8.2 Phân tích rủi ro

Phân tích rủi ro xây dựng mức toàn vẹn được yêu cầu cho toàn bộ hệ thống. Phân tích rủi ro là một quy trình liên tục và lặp nhằm cân bằng giữa điều chưa thể biết với điều cần được biết. Các mức toàn vẹn phát sinh từ việc phân tích rủi ro là một chuyển đổi các giá trị hệ quả thành sự xuất hiện và điều chỉnh điều kiện hoặc hành vi hệ thống. Sự chuyển đổi này được lan truyền theo các mức toàn vẹn bên trong hệ thống và của các phụ thuộc của chính chúng cũng theo sự xuất hiện và định thời. Do vậy, mức toàn vẹn là một sự lập điều lệ của điều cần được hoàn thành và được thể hiện cho nhiều dải và điều kiện khó khăn của giới hạn dựa trên giá trị đặc tính và độ không xác định đi kèm của chúng.

Bộ TCVN 10607 không bao gồm việc phân tích rủi ro chi tiết. Nhiều tiêu chuẩn và tài liệu hướng dẫn hiện hành đưa ra các hướng dẫn cho việc phân tích rủi ro và có thể hỗ trợ trong việc định danh các hệ quả tiêu cực tiềm ẩn. IEC 61508 [70] và IEC 31010 phiên bản 1.0 (27/11/2009) *Risk management - Risk management techniques*, đưa ra các cách tiếp cận cho việc phân tích rủi ro. Thuật ngữ đặc trưng về an toàn - được dùng trong IEC 300-3-9, thuật ngữ "độc hại" và "tổn hại" nên được phiên dịch thành "điều kiện nguy hiểm" và "hệ quả tiêu cực". IEC 60300 *Dependability management* [64] cũng đưa ra hướng dẫn.

Các tiêu chuẩn viện dẫn bao gồm: ISO 13849 [78] về Dây chuyền. ISS 14620 [79] về Hệ thống không gian, ISO 19706 [81] về Lửa, ISO/TS 25238 [121] về Thông tin sức khỏe, ISO/EC 27005 [111] về An ninh thông tin và UK CAP 760 về Hàng không và Giao thông hàng không. Điều cũng đáng quan tâm là các tiêu chuẩn quản lý rủi ro phổ biến hơn, ví dụ: ISO/IEC 16085 [91] và ISO 31000.

9 Bộ TCVN 10607 và vòng đời

9.1 Giới thiệu

TCVN 10607-4 *Đảm bảo trong vòng đời* đưa ra một *dạng quy trình* cho việc đảm bảo hệ thống và phần mềm bằng cách đưa ra một mô tả mục đích và một tập kết quả phù hợp cho việc đảm bảo hệ thống và phần mềm. Khái niệm *dạng quy trình* được hình thành và mô tả trong phụ lục của ISO/IEC 15288 *Systems and software engineering - System life cycle processes*. Như một quy trình, việc mô tả dạng quy trình bao gồm một mô tả mục đích và các kết quả. Không giống một quy trình, việc mô tả một dạng quy trình không bao gồm các hoạt động và tác vụ. Thay vào đó, việc mô tả bao gồm hướng dẫn và các khuyến nghị giải thích cách thức mà các kết quả có thể đạt được bằng cách thực hiện các hoạt động và tác vụ của nhiều quy trình trong hai tiêu chuẩn: ISO/IEC 15288 và ISO/IEC 12207 *Systems and software engineering - Software life cycle processes*.

Tất cả các quy trình vòng đời được mô tả trong cả hai tiêu chuẩn: ISO/IEC 15288 và ISO/IEC 12207 mặc dù các quy trình trong ISO/IEC 12207 được đặc trưng cho phần mềm và trong một vài trường hợp có nhiều tên gọi khác nhau phản ánh đặc trưng đó. ISO/IEC 12207 bao gồm các quy trình không được nói đến trong ISO/IEC 15288, liên quan tới các quy trình xây dựng phần mềm, quy trình hỗ trợ và các quy trình tái sử dụng.

Tất cả các quy trình, hoạt động, tác vụ và hướng dẫn và các khuyến nghị phải được thực hiện trong ngữ cảnh của một mô hình vòng đời. Báo cáo kỹ thuật nhiều phần ISO/IEC/TR 24748 *Systems and software engineering - Life cycle management* được thiết kế nhằm tạo cơ hội cho việc sử dụng kết hợp nội dung quy trình của hai tiêu chuẩn quy trình vòng đời. ISO/IEC/TR 24748 đưa ra hướng dẫn thống nhất và kiện toàn về quản lý vòng đời hệ thống và phần mềm. Mục đích của tiêu chuẩn này nhằm giúp đảm bảo tính toàn vẹn trong các khái niệm hệ thống và vòng đời, các mô hình, giai đoạn, quy trình, ứng dụng quy trình, sự lặp và đệ quy của các quy trình trong suốt vòng đời, các quan điểm chủ đạo, sự chấp thuận và sử dụng trong nhiều lĩnh vực. ISO/IEC 24748-1 minh họa việc sử dụng một mô hình vòng đời cho các hệ thống đặt trong ngữ cảnh của ISO/IEC 15288 và đưa ra một minh họa tương ứng cho việc sử dụng một mô hình vòng đời trong ngữ cảnh của ISO/IEC 12207.

TCVN 10607-4 đưa ra cho người dùng sự tự do lựa chọn dù họ sử dụng một tạo tác cụ thể được gọi là một "trường hợp đảm bảo" hoặc văn bản hóa thông tin đảm bảo liên quan trong các tài liệu khác. Vấn đề là để đạt được đòi hỏi mức cao và sau đó thể hiện việc đạt được đòi hỏi cho giá trị của một đặc tính quan trọng cho một bên liên quan tương ứng. Các quy trình vòng đời, hoạt động và các tác vụ cần phản ánh nhằm nhận diện một hệ thống tương ứng và được chắc chắn rằng hệ thống là tương ứng bằng cách thể hiện việc đạt được sự tin tưởng được yêu cầu của các bên liên quan.

Người dùng TCVN 10607-4 có thể yêu cầu việc đánh giá và quản lý rủi ro, phép đo và các yêu cầu quy trình hoàn toàn được xây dựng đầy đủ hơn các xử lý được nêu trong hai tiêu chuẩn: ISO/IEC 15288 và ISO/IEC 12207. Ba tiêu chuẩn: ISO/IEC 16085 *Risk management*, ISO/IEC 15939 *Measurement* và ISO/IEC/IEEE 29148 *Requirements engineering* được thiết kế để sử dụng với hai tiêu chuẩn: ISO/IEC 15288 và ISO/IEC 12207 nhằm cung cấp một cách chi tiết hơn cho ba quy trình này. Các tiêu chuẩn khác đưa ra các yêu cầu và hướng dẫn hữu ích cho các quy trình được chọn lựa trong hai tiêu chuẩn: ISO/IEC/IEEE 15289 cho tài liệu hóa phát sinh từ việc thực hiện các quy trình vòng đời và ISO/IEC/IEEE 16326 cho quy trình quản lý dự án.

Bộ tiêu chuẩn này được thiết kế nhằm tương thích với các tiêu chuẩn quy trình vòng đời này. Mục tiêu của việc đảm bảo, việc chọn lựa các đòi hỏi được đảm bảo, lập kế hoạch đảm bảo liên quan, xây dựng và duy trì trường hợp đảm bảo có các ảnh hưởng trong tất cả quy trình vòng đời.

9.2 Hoạt động đảm bảo trong vòng đời

Việc thực hiện một tập các hoạt động đảm bảo theo hệ thống và kế hoạch là cần thiết nhằm cung cấp các cơ sở cho sự tin tưởng theo các đặc tính hệ thống. Các hoạt động này được thiết kế nhằm đảm bảo rằng cả quy trình và hệ thống phù hợp với các đòi hỏi, tiêu chuẩn, hướng dẫn và các thủ tục đã được định nghĩa của chúng. "Quy trình" trong ngữ cảnh này, bao gồm tất cả các hoạt động liên quan trong việc thiết kế, phát triển và duy trì của hệ thống. Với phần mềm, "sản phẩm phần mềm" bao gồm chính các phần mềm đó, dữ liệu liên quan tới nó, tài liệu của nó, việc hỗ trợ và các tư liệu báo cáo được cung cấp như một phần của quy trình phần mềm (ví dụ: các kết quả thử nghiệm và lập luận đảm bảo) cũng như điều gì cần thiết để hoàn thiện trường hợp đảm bảo. "Yêu cầu" bao gồm yêu cầu của các đặc tính cần được đưa ra, chủ yếu dựa theo các yêu cầu nhằm giới hạn, giảm thiểu hoặc quản lý các chi phí liên quan tới đặc tính và các tổn thất. "Tiêu chuẩn và hướng dẫn" có thể là kỹ thuật xác định

các công nghệ có thể được sử dụng trong hệ thống hay phần mềm, hoặc có thể là phi công nghệ xác định các khía cạnh của quy trình mà được mô tả nhiều hơn bởi “thủ tục” nhằm thỏa mãn các yêu cầu hệ thống có thể xảy ra.

Việc quản lý các hoạt động vòng đời bao gồm việc quản lý các hoạt động liên quan trực tiếp tới thông tin đảm bảo liên quan và ảnh hưởng mà thông tin đảm bảo liên quan có trong các hoạt động khác. Việc quản lý này được thực hiện tốt nhất khi các đòi hỏi mức cao được xem xét từ lúc bắt đầu phát triển khái niệm, được sử dụng nhằm ảnh hưởng tới tất cả hoạt động và hệ thống [140] và Phụ lục B trong [22], trở thành một phần không thể thiếu của toàn bộ quy trình kỹ thuật. Các hoạt động này có thể được hoàn thiện hoàn toàn chỉ khi hệ thống và nội dung thông tin thể hiện việc đạt được các đòi hỏi đó được phát triển một cách đồng thời.

Bản chất song hành của việc phát triển lý do và lập luận này cũng là một trong những lợi ích của việc phát triển đồng thời của hệ thống và trường hợp đảm bảo của nó. Quy trình phát triển và hệ thống có thể nhằm mục đích không chỉ đạt được đòi hỏi mà còn thực hiện theo một cách thức thể hiện tương ứng bởi trường hợp đảm bảo. Trường hợp đảm bảo tác động tới hệ thống bằng cách làm cho nó phát triển theo cách thức mà một lập luận thực tế hơn để xây dựng. Trường hợp đảm bảo này thường tạo ra một hệ thống đơn giản hơn (ít nhất là nội bộ), một hệ thống mà các phần tử hệ thống có thể được sử dụng riêng biệt nhằm thể hiện những đòi hỏi phụ nhất định và một sự phân bổ các khía cạnh của hệ thống như lý do hợp nhất của trạng thái kỹ thuật và thực tế. Các quy trình đồng thời có thể bao gồm các yêu cầu bao trùm nhiều điều kiện và sự kiện hơn cũng như khả năng phục hồi tương ứng, các phương pháp được sử dụng nhằm tạo ra ít lỗi hơn và việc hiệu chỉnh hay xác thực được nhắm tới điều cần thiết được thể hiện và việc thể hiện một cách thích hợp.

10 Tổng kết

Tiêu chuẩn này được viết nhằm cung cấp cho người dùng tất cả các phần của bộ tiêu chuẩn này một kiến thức tương đối về các khái niệm và thuật ngữ được sử dụng trong bộ tiêu chuẩn này mà trước đây có thể không được chia sẻ thông qua các cộng đồng được phục vụ. Các giải thích về điều được bao trùm trong mỗi phần của bộ tiêu chuẩn này cần cung cấp một cơ sở cho việc lựa chọn và sử dụng các phần đó, cũng như một lý do tiềm ẩn của cấu trúc của chính bộ tiêu chuẩn này.

Thư mục tài liệu tham khảo

[1] Abra A., Moore J.W. (Executive editors); Pierre Bourque, Robert Dupuis, Leonard Tripp (Editors). Guide to the Software Engineering Body of Knowledge. phiên bản 2004. Los Alamitos, California:IEEE Computer Society, 16 tháng Hai 2004. Có sẵn tại: http://www.swebok.org

[2] Adamski A., Westrum R. Requisite imagination:The fine art of anticipating what might go wrong." Trong:[55], từ trang 193-220, 2003

[3] Adelard. The Adelard Safety Case Development Manual. Có sẵn tại: http://www.adelard.com/web/hnav/resources/ascad

[4] Alexander | *Systems Engineering Isn't Just Software*. 2001. Có sẵn tại: http://easyweb.easynet.co.uk/~iany/consultancy/systems_engineering/se_isnt_just_sw.htm

[5] J.H. Allen, S. Barum, R.J. Ellison, G. McGraw, N.R. Mead. *Software Security Engineering:A Guide for Project Managers*. Addison-Wesley, 2008

[6] W. Altman, T. Ankrum, W. Brach. *Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants:A Report to Congress*. U.S. Nuclear Regulatory Commission:Office of Inspection and Enforcement, 1987

[7] J.P Anderson *Computer Security Technology Planning Study Volume I*, ESDTR-73-51, Vol. I, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01730, tháng Mười 1972

[8] R.J. Anderson *Security Engineering:A Guide to Building Dependable Distributed Systems.* John Wiley and Sons, xuất bản lần 2, 2008

[9] T.S. Ankrum, A.H. Kromholz. Structured Assurance Cases:Three Common Standards," Ninth IEEE International Symposium on High-Assurance Systems Engineering (HASE'05), từ trang 99-108, 2005

[10] J.M. Armstrong, S.P Paynter *The Deconstruction of Safety Arguments through Adversarial Counter-argument*. School of Computing Science, Newcastle University CS-TR-832, 2004

[11] B. Atchison, P. Lindsay, D. Tombs *A Case Study in Software Safety Assurance Using Formal Methods*. Technical Report No. 99-31. tháng Chín 1999

[12] ATSIN Number 17 Issued 9. Lapses and Mistakes. Air Traffic Services Information Notice, Safety Regulation Group, ATS Standards Department. UK Civil Aviation Authority, tháng Tám 2002

[13] A.T. Bahill, B. Gissing Re-evaluating Systems Engineering Concepts Using Systems Thinking. *IEEE Trans. Syst. Man Cybern. C*, tháng Mười một 1998, 28 (4) từ trang 516-527

[14] C.J. Berg *High-Assurance Design: Architecting Secure and Reliable Enterprise Applications*. Addison Wesley, 2006

[15] Lawrence Bernstein, C. M. Yuhas Trustworthy Systems through Quantitative Software Engineering. Wiley-IEEE Computer Society Press, 2005. Về độ tin cậy không an toàn

[16] M. Bishop, S. Engle *The Software Assurance CBK and University Curricula*. Proceedings of the 10th Colloquium for Information Systems Security Education, 2006

[17] M. Bishop *Computer Security:Art and Practice*. Addison-Wesley, 2003

[18] P Bishop, R. Bloomfield *A Methodology for Safety Case Development*. Industrial Perspectives of Safety-critical Systems:Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham. 1998

[19] P Bishop, R. Bloomfield *The SHIP Safety Case Approach*. SafeComp95, Belgirate, Italy. Tháng Mười 1995

[20] M.J. Buehner, P.W. Cheng Causal Learning. Trong:*The Cambridge Handbook of Thinking and Reasoning*, (R. Morrison, K.J. Holyoak eds.). Cambridge University Press, 2005, từ trang 143-68

[21] J.C. Cannon. *Privacy*. Addison Wesley, 2005

[22] CAP 670 Air Traffic Services Safety Requirements. UK Civil Aviation Authority Safety Regulation Group, 2012

[23] CAP 730 Safety Management Systems for Air Traffic Management A Guide to Implementation. UK Civil Aviation Authority Safety Regulation Group, 12 tháng Chín 2002

[24] 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, 10 tháng Mười hai 2010

[25] L. Chung *Non-Functional Requirements in Software Engineering*. Kluwer, 1999

[26] D.D. Clark, D.R. Wilson *A Comparison of Commercial and Military Computer Security Policies*, Proc. of the 1987 IEEE Symposium on Security and Privacy, IEEE, từ trang 184-196, 1987

[27] CNSS National Information Assurance Glossary, CNSS Instruction No. 4009, 26 tháng Tư 2010. Có sẵn tại: http://www.cnss.gov/full-index.html

[28] Committee on Information Systems Trustworthiness *Trust in Cyberspace, Computer Science and Telecommunications Board*. National Research Council, 1999

[29] Committee on National Security Systems (CNSS) Instruction 4009:National Information Assurance (IA) Glossary. Soát xét tháng Năm 2003. Có sẵn tại: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[30] Common Criteria Recognition Arrangement (CCRA) Common Criteria v3.1 Revision 2. NIAP tháng Chín 2007. Có sẵn tại: http://www.commoncriteriaportal.org

[31] Common Weaknesses Enumeration MITRE, 2012. Có sẵn tại: http://cwe.mitre.org

[32] N.J. Cooke, J.C. Gorman, J.L. Winner Team Cogitation. từ trang 239-268 Trong:[43]

[33] P.-J. Courtois *Justifying the Dependability of Computer-based Systems:With Applications in Nuclear Engineering*. Springer, 2008

[34] L. Cranor, S. Garfinkel *Security and Usability:Designing Secure Systems that People Can Use*. O'Reilly, 2005

[35] Dayton-Johnson. Jeff. Natural disasters and adaptive capacity. OECD Development Centre Research programme on:Market Access, Capacity Building and Competitiveness. Working Paper No. 237 DEV/DOC(2004)06, tháng Tám 2004

[36] Department of Defense Directive 8500.1 (6 tháng Hai 2003). Information Assurance (IA), Washington, DC:US Department of Defense, ASD(NII)/DoD CIO, 23 tháng Tư, 2007. Có sẵn tại: http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

[37] Department of Defense Strategic Defense Initiative Organization. Trusted Software Development Methodology, SDI-S-SD-91-000007, vol. 1, 17 tháng Sáu 1992

[38] Department of Homeland Security National Cyber Security Division's "Build Security In" (BSI) web site, 2012, http://buildsecurityin.us-cert.gov

[39] Dependability Research Group *Safety Cases*. University of Virginia, Có sẵn tại: http://dependability.cs.virginia.edu/info/Safety_Cases

[40] G. Despotou, T. Kelly *Extending the Safety Case Concept to Address Dependability*, Proceedings of the 22nd International System Safety Conference, 2004

[41] M. Dowd, J. McDonald, J. Schuh *The Art of Software Security Assessment:Identifying and Preventing Software Vulnerabilities*. Addison-Wesley, 2006

[42] K. Dunbar, J. Fugelsang Scientific Thinking and Reasoning. Trong:[59], từ trang 705-727

[43] F.T. Durso, R.S. Nickerson, S.T. Dumais, S. Lewandowsky, T.J. Perfect eds. *Handbook of Applied Cognition* xuất bản lần 2, Wiley, 2007

[44] P.C. Ellsworth Legal Reasoning. Trong:[59], từ trang 685-704

[45] K.A. Ericsson, N. Charness, P.J. Feltovich, R.R. Hoffman eds. *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press, 2006

[46] N. Fenton, B. Littlewood, M. Neil, L. Strigini, A. Sutcliffe, D. Wright Assessing dependability of safety critical systems using diverse evidence. *IEE Proc. Softw*. 1998 145 (1) từ trang 35-39

[47] M. Gasser Building a Secure Computer System. Van Nostrand Reinhold, 1988. Có sẵn tại: http://deke.ruc.edu.cn/wshi/readings/cs02.pdf

[48] J.W. Gray *Probabilistic Interference*. Proceedings of the IEEE Symposium on Research in Security and Privacy. IEEE, từ trang 170-179, 1990

[49] W. Greenwell, E. Strunk, J. Knight *Failure Analysis and the Safety-Case Lifecycle*. IFIP Working Conference on Human Error, Safety and System Development (HESSD) Toulouse, France, tháng Tám 2004

[50] W.S. Greenwell, J.C. Knight, J.J. Pease *A Taxonomy of Fallacies in System Safety Arguments*. 24th International System Safety Conference, Albuquerque, NM, tháng Tám 2006

[51] A. Hall, R. Chapman Correctness by Construction:Developing a Commercial Secure System. *IEEE Softw*. 2002 Jan/Feb, 19 (1) từ trang 18-25

[52] D.S. Herrmann *Software Safety and Reliability*. IEEE Computer Society Press, 1999

[53] G. Hoglund, G. McGraw *Exploiting Software:How to break code*. Addison-Wesley, 2004

[54] E. Hollnagel, D.D. Woods, N. Leveson eds. *Resilience Engineering:Concepts and Precepts*. Ashgate Pub Co, 2006

[55] E. Hollnagel ed. *Handbook of cognitive task design*. Lawrence Erlbaum Associates, 2003

[56] E. Hollnagel Human Error:Trick or Treat?. Trong:[43], từ trang 219-238

[57] E. Hollnagel *Barriers and Accident Prevention*. Ashgate, 2004

[58] E. Hollnagel Human Factors:From Liability to Asset. Presentation, 2007. Có sẵn tại: www.vtt.fi/liitetiedostot/muut/Hollnagel.pdf

[59] K.J. Holyoak, R.G. Morrison eds. *The Cambridge Handbook of Thinking and Reasoning*. Cambridge University Press, 2005

[60] M. Howard, D.C. LeBlanc *Writing Secure Code*. Microsoft Press, xuất bản lần 2, 2002

[61] M. Howard, S. Lipner *The Security Development Lifecycle*. Microsoft Press, 2006

[62] C. Howell Assurance Cases for Security Workshop (follow-on workshop of the 2004 Symposium on Dependable Systems and Networks), tháng Sáu 2005

[63] IEC 60050-191, *International Electrotechnical Vocabulary, Chapter 191: Dependability and Quality of Service*

[64] IEC 60300 *Dependability management* [vài phần]

[65] IEC 60300-3-15 ed1.0 (2009-06) Dependability management - Part 3-15 - Application guide - Engineering of system dependability

[66] IEC 60300-3-2 ed.2.0 (2004-11), *Dependability management - Part 3-2:Application guide - Collection of dependability data from the field*

[67] IEC 60812 ed2.0 (2006-01), *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*

[68] IEC 61025 ed2.0 (2006-12), *Fault tree analysis (FTA)*

[69] IEC 61078 ed2.0 (2006-01), *Analysis techniques for dependability - Reliability block diagram and Boolean methods*

[70] IEC 61508 ed2.0, *Functional safety of electrical/electronic/programmable electronic safety-related systems* [vài phần]

[71] IEC 61508-7 ed2.0 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7:Overview of techniques and measures*

[72] IEC 61511 ed1.0, *Functional safety - Safety instrumented systems for the process industry sector* [vài phần]

[73] IEC 61882 ed1.0 (2001-05), *Hazard and operability studies (HAZOP studies) - Application guide*

[74] IEC CD 62741 ed.1.0, *Reliability of systems, equipment, and components. Guide to the demonstration of dependability requirements. The dependability case*

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

[76] International Council on Systems Engineering INCOSE Guide to Systems Engineering Body of Knowledge (G2SEBoK). Có sẵn tại: http://g2sebok.incose.org/

[77] ISO 12100:2010, *Safety of machinery - General principles for design - Risk assessment and risk reduction*

[78] ISO 13849, *Safety of machinery - Safety-related parts of control systems* [ba phần]

[79] ISO 14620, *Space systems - Safety requirements* [ba phần]

[80] ISO 14625:2007, *Space systems - Ground support equipment for use at launch, landing or retrieval sites - General requirements*

[81] ISO 19706:2011, *Guidelines for assessing the fire threat to people*

[82] ISO 20282, *Ease of operation of everyday products* [bốn phần]

[83] ISO 2394:1998, *General principles on reliability for structures*

[84] ISO 28003:2007, *Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems*

[85] ISO 9241-400:2007, *Ergonomics of human - system interaction - Part 400:Principles and requirements for physical input devices*

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

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

[88] ISO/IEC 15408, *Information technology - Security techniques - Evaluation criteria for IT security* [ba phần]

[89] ISO/IEC TR 15443, *Information technology - Security techniques - Security assurance framework* [hai phần]

[90] ISO/IEC 15939:2007, *Systems and software engineering - Measurement process*

[91] ISO/IEC 16085:2006, *Systems and software engineering - Life cycle processes - Risk Management*

[92] ISO/IEC/IEEE 16326:2009, *Systems and software engineering - Life cycle management - Project management*

[93] ISO/IEC 18014, *Information technology - Security techniques - Time-stamping services* [ba phần]

[94] ISO/IEC 18028, *Information technology - Security techniques - IT network security* [nhiều phần]

[95] ISO/IEC 19770, *Information technology - Software Asset Management* [hai phần]

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

[97] ISO/IEC 2382-14:1997, *Information technology - Vocabulary - Part 14:Reliability, maintainability and availability*

[98] ISO/IEC 25000:2005, *Software Engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Guide to SquaRE*

[99] ISO/IEC 25010:2011, *Systems and software engineering - Systems and software product Quality Requirements and Evaluation (SQuaRE) - System and software quality models*

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

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

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

[103] ISO/IEC 25040:2011, *Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Evaluation process*

[104] 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*

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

[106] ISO/IEC 27000:2012, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

[107] ISO/IEC 27001:2013, *Information technology - Security techniques - Information security management systems – Requirements*

[108] ISO/IEC 27002:2013, *Information technology - Security techniques - Code of practice for information security controls*

[109] ISO/IEC 27004:2009, *Information technology - Security techniques - Information security management – Measurement*

[110] ISO/IEC 27005:2011, *Information technology - Security techniques - Information security risk management*

[111] ISO/IEC 27006:2011, *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*

[112] ISO/IEC 27011:2008, *Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[113] ISO/IEC/IEEE 42010:2011, *Systems and software engineering - Architecture Description*

[114] ISO/IEC 90003:2004, *Software engineering - Guidelines for the application of ISO 9001:2000 to computer software*

[115] ISO/IEC TR 15446:2009, *Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets*

[116] ISO/IEC TR 19791:2010, *Information technology - Security techniques - Security assessment of operational systems*

[117] ISO/IEC TR 24748-1:2010, *Systems and software engineering - Life cycle management - Part 1:Guide for life cycle management*

[118] ISO/TR 16982:2002, *Ergonomics of human-system interaction - Usability methods supporting human-centred design*

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

[120] ISO/TR 27809:2007, *Health informatics - Measures for ensuring patient safety of health software*

[121] ISO/TS 25238:2007, *Health informatics - Classification of safety risks from health software*

[122] R. Kazman, J. Asundi, M. Klein *Making Architecture Design Decisions:An Economic Approach*, SEI-2002-TR-035. Software Engineering Institute, Carnegie Mellon University, 2002

[123] R. Kazman, M. Klein, pp. Clements ATAM:Method for Architecture Evaluating the Quality Attributes of a Software Architecture. Technical Report CMU/SEI-200-TR004. Software Engineering Institute, Carnegie Mellon University, 2000

[124] T. Kelly *Arguing Safety - A Systematic Approach to Managing Safety Cases*. Doctorial Thesis - University of York:Department of Computer Science, tháng Chín 1998

[125] T. Kelly *Reviewing Assurance Arguments - A Step-by-Step Approach*. Workshop on Assurance Cases for Security:The Metrics Challenge, International Conference on Dependable Systems and Networks, 2007

[126] T. Kelly, R. Weaver *The Goal Structuring Notation - A Safety Argument Notation*. Workshop on Assurance Cases:Best Practices, Possible Obstacles, and Future Opportunities, Florence, Italy, tháng Bảy 2004

[127] P. Ladkin *The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed*. 29 tháng Tám 2002. Có sẵn tại: http://www.rvs.uni-bielefeld.de/publications/Reports/SCflawed-paper.html

[128] C. Landwehr Computer Security. *IJIS*. 2001, 1 từ trang 3-13

[129] S. Lautieri, D. Cooper, D. Jackson *SafSec:Commonalities Between Safety and Security Assurance*. Proceedings of the Thirteenth Safety Critical Systems Symposium - Southampton, 2005

[130] R.A. LeBoeuf, E.B. Shafir Decision Making. Trong:[59], từ trang 243-266

[131] N. Leveson A Systems-Theoretic Approach to Safety in Software-Intensive Systems, *IEEE Trans. Dependable Sec. Comput*. 2004, 1 (1) từ trang 66-86

[132] S. Lipner, M. Howard *The Trustworthy Computing Security Development Lifecycle*, Microsoft, 2005. Có sẵn tại: http://msdn.microsoft.com/en-us/library/ms995349.aspx

[133] R. Maguire *Safety Cases abd Safety Reports:Meaning, Motivation and Management*. Ashgate, 2006

[134] J. McDermid *Software Safety:Where's the Evidence?* 6th Australian Workshop on Industrial Experience with Safety Critical Systems and Software (SCS '01), Brisbane. 2001

[135] G. McGraw *Software Security:Building Security In*. Addison Wesley, 2006

[136] J. McLean Security Models. Trong:*Encyclopedia of Software Engineering*, (J. Marciniak ed.). Wiley, 1994

[137] J.D. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamilla, Murukan A. *Improving Web Application Security:Threats and Countermeasures*, Microsoft, 2004. Có sẵn tại: http://download.microsoft.com/download/d/8/c/d8c02f31-64af-438c-a9f4-e31acb8e3333/Threats_Countermeasures.pdf

[138] M.S. Merkow, J. Breithaupt *Computer Security Assurance Using the Common Criteria*. Thompson Delamr Learning, 2005

[139] 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

[140] Ministry Of Defence. Defence Standard 00-55 (PART 1)/Issue 2, Requirements for Safety Related Software in Defence Equipment Part 1:Requirements, 21 tháng Tám 1997

[141] 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

[142] Ministry of Defence. Interim Defence Standard 00-56, Safety Management Requirements for Defence Systems Part 1:Requirements, 17 tháng Mười hai 2004

[143] Ministry of Defence. Interim Defence Standard 00-56, Safety Management Requirements for Defence Systems Part 2:Guidance on Establishing a Means of Complying with Part 1, 17 tháng Mười hai 2004

[144] A. Moore, E. Klinker, D. Mihelcic How to Construct Formal Arguments that Persuade Certifiers. Trong:*Industrial Strength Formal Methods in Practice*. Academic Press. 1999

[145] National Aeronautics and Space Administration (NASA) Software Assurance Guidebook tháng Chín 1989 (NASA-GB-A201). Có sẵn tại: http://www.hq.nasa.gov/office/codeq/doctree/nasa_gb_a201.pdf

[146] National Offshore Petroleum Safety Authority Safety case. [Online Documents [cited on:20 tháng Sáu 2012]. Có sẵn tại: http://www.nopsema.gov.au/safety/safety-case/

[147] National Research Council (NRC) Computer Science and Telecommunications Board (CSTB). Cybersecurity Today and Tomorrow:Pay Now or Pay Later. National Academies Press, 2002. Có sẵn tại: http://www.nap.edu/topics.php?topic=320&start=10

[148] National Security Agency, The Information Systems Security Engineering Process (IATF) v3.1. 2002

[149] Naval Research Laboratory *Handbook for the Computer Security Certification of Trusted Systems*. US Naval Research Laboratory, 1995

[150] NDIA System Assurance Committee *Engineering for System Assurance*. National Defense Industrial Association, USA, 2008

[151] NIST Federal Information Processing Standards Publication (FIPS PUB) 200:Minimum Security Requirements for Federal Information and Information Systems. March 2006. Có sẵn tại: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[152] NIST NIST Special Publication 800-27, Rev A:Engineering Principles for Information Technology Security (A Baseline for Achieving Security). Revision A, tháng Sáu 2004. Có sẵn tại: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

[153] NIST NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security, tháng Mười hai 2001. Có sẵn tại: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

[154] Process Framework O.P.E.N. Safety Cases. [Online Document cited on: 20 tháng Sáu 2012].

Có sẵn tại:
http://www.opfro.org/index.html?Components/WorkProducts/SafetySet/SafetySet.html~Contents

[155] OPSI The Offshore Installations (Safety Case) Regulations 2005. [Online Document cited on: 20 tháng Sáu 2012.] Có sẵn tại: http://www.opsi.gov.uk/si/si2005/20053117.htm

[156] J. Park, B. Montrose, J. Froscher *Tools for Information Security Assurance Arguments*. *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01*. Proceedings, 2001

[157] H. Petroski *Design Paradigms*. Cambridge University Press, 1994

[158] D. Prasad *Dependable Systems Integration using Measurement Theory and Decision Analysis*, PhD Thesis, Department of Computer Science, University of York, UK, 1998

[159] PSM Safety & Security TWG. *Security Measurement*, tháng Mười một 2004

[160] L.L. Pullum *Software Fault Tolerance*. Artech House, 2001

[161] B. Randell, M. Koutny Failures:Their Definition, Modelling and Analysis. School of Computing Science, Newcastle University CS-TR NO 994, tháng Mười hai 2006B. Randell, J.M. Rushby Distributed Secure Systems: Then and Now. CS-TR No 1052 School of Computing Science, Newcastle University, tháng Mười 2007

[162] E. Rechtin *Systems Architecting of Organizations:Why Eagles Can't Swim*. CRC Press, Boca Raton, FL, 2000

[163] S.T. Redwine Jr. ed. *Software Assurance:A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software Version 1.1*. US Department of Homeland Security, tháng Chín 2006

[164] S.T. Redwine Jr. *The Quality of Assurance Cases*. Workshop on Assurance Cases for Security:The Metrics Challenge, International Conference on Dependable Systems and Networks, 2007

[165] S.T. Redwine Jr., N. Davis eds. Processes for Producing Secure Software:Towards Secure Software. Vols. I and II. Washington, D.C.:National Cyber Security Partnership, 2004. Có sẵn tại: http://www.cigital.com/papers/download/secure_software_process.pdf

[166] K.G. Ross, J.L. Shafer, G. Klein Professional Judgements and 'Naturalistic Decision Making'. Trong: [45], trang 403-420

[167] R. Ross Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, tháng Tám 2009. Có sẵn tại: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[168] SAE JA1000, *Reliability Program Standard, SAE International*, tháng Sáu 1998. Có sẵn tại: http://www.sae.org

[169] J.H. Saltzer, M.D. Schroeder The protection of information in computer systems. Proc. IEEE. 1975, 63 (9) từ trang 1278-1308. Có sẵn tại: http://cap-lore.com/CapTheory/ProtInf/

[170] Seminal Papers - History of Computer Security Project, University of California Davis Computer Security Laboratory. Có sẵn tại: http://seclab.cs.ucdavis.edu/projects/history/seminal.html

[171] Serene. "Safety argument." [Online Document] [cited on:13 Feb 2007] Có sẵn tại: http://www2.dcs.qmul.ac.uk/~norman/SERENE_Help/sereneSafety_argument.htm

[172] K. Severson *Yucca Mountain Safety Case Focus of NWTRB September Meeting*. United States Nuclear Waste Technical Review Board, tháng Tám 2006

[173] W.R. Sieck, G. Klein Decision making. Trong:[43], từ trang 195-218

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

[175] I. Sommerville *Software Engineering*. Pearson Education, xuất bản lần 8, 2006

[176] G. Stoneburner, C. Hayden, A. Feringa *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Revision A, NIST Special Publication 800-27 Rev A, tháng Sáu 2004

[177] N. Storey *Safety-Critical Computer Systems*. Addison Wesley, 1996

[178] E. Strunk, J. Knight *The Essential Synthesis of Problem Frames and Assurance Cases*. IWAAPF'06, Shanghai, China, tháng Năm 2006

[179] F. Swiderski, W. Snyder *Threat Modeling*. Microsoft Press, 2004

[180] U.S. NRC. "Quality Assurance Case Studies at Construction Projects."

[181] W.M. Vanfleet MILS:Architecture for High Assurance Embedded Computing," Crosstalk, tháng Tám, 2005

[182] J. Viega, G. McGraw *Building Secure Software:How to Avoid Security Problems the Right Way*. Addison Wesley, Reading, MA, 2001

[183] V.R. Walker Risk Regulation and the 'Faces' of Uncertainty, *Risk:Health, Safety and Environment*. từ trang 27-38, mùa đông 1998

[184] W.H. Ware Security Controls for Computer Systems (U):Report of Defense Science Board Task Force on Computer Security, The RAND Corporation, Santa Monica, CA (tháng Hai 1970)

[185] R. Weaver *The Safety of Software - Constructing and Assuring Arguments*. Doctorial Thesis - University of York:Department of Computer Science. 2003

[186] R. Weaver, J. Fenn, T. Kelly A *Pragmatic Approach to Reasoning about the Assurance of Safety Arguments*. 8th Australian Workshop on Safety Critical Systems and Software (SCS'03), Canberra. 2003

[187] J.A. Whittaker, H.H. Thompson *How to Break Software Security:Effective Techniques for Security Testing*. Pearson Education, 2004

[188] J. Williams, M. Schaefer *Pretty Good Assurance*. Proceedings of the New Security Paradigms Workshop. IEEE Computer Society Press. 1995

[189] J.R. Williams, G.F. Jelen *A Framework for Reasoning about Assurance*, Document Number ATR 97043, Arca Systems, Inc., 23 tháng Tư 1998

[190] J.F. Yates, M.D. Tschirhart Decision-Making Expertise. Trong: [45], từ trang 421 tới 438

[191] K.-P. Yee *User interaction design for secure systems*. Proceedings of the 4th International Conference on Information and Communications Security, Springer-Verlag, LNCS 2513, 2002