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

TCVN 10607-3:2014
ISO/IEC 15026-3:2011

Xuất bản lần 1

KỸ THUẬT PHẦN MỀM VÀ HỆ THỐNG – ĐẢM BẢO PHẦN MỀM VÀ HỆ THỐNG – PHẦN 3: MỨC TOÀN VẸN HỆ THỐNG

Systems and software engineering **–**
Systems and software assurance **–**
Part 3: System integrity levels

HÀ NỘI – 2014

Mục lục **Trang**

Lời nói đầu

TCVN 10607-3:2014 hoàn toàn tương đương với ISO/IEC 15026-3:2011**.**

TCVN 10607-3:2014 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 3: Mức toàn vẹn hệ thống

Systems and software engineering – Systems and software assurance –

Part 3: System integrity levels

1 Phạm vi áp dụng

Tiêu chuẩn này quy định khái niệm về mức toàn vẹn theo yêu cầu tương ứng với mức toàn vẹn được yêu cầu nhằm chỉ ra việc đạt được mức toàn vẹn. Tiêu chuẩn này đặt ra các yêu cầu và khuyến nghị các phương pháp nhằm định nghĩa, sử dụng mức toàn vẹn và các yêu cầu mức toàn vẹn của chúng. Tiêu chuẩn này bao trùm các hệ thống, sản phẩm phần mềm và các thành phần của chúng, cũng như các phụ thuộc bên ngoài liên quan.

Tiêu chuẩn này có thể áp dụng cho các hệ thống và phần mềm, được sử dụng bởi:

a) Người định nghĩa các mức toàn vẹn, ví dụ: các tổ chức chuyên gia và công nghiệp, tổ chức tiêu chuẩn và cơ quan chính phủ;

b) Người dùng mức toàn vẹn, ví dụ: nhà phát triển, nhà bảo trì, nhà cung cấp, nhà thâu nhận, người dùng, đánh giá viên hệ thống hay phần mềm và cho việc quản trị và hỗ trợ kỹ thuật của các hệ thống và/hoặc sản phẩm phần mềm.

Cách sử dụng quan trọng của mức toàn vẹn là các thỏa thuận giữa nhà cung cấp và nhà thâu nhận, ví dụ: nhằm hỗ trợ việc đảm bảo an toàn, tiết kiệm hoặc các thuộc tính an ninh của một sản phẩm hay hệ thống được phân phối.

Tiêu chuẩn này không liệt kê một tập mức toàn vẹn hay yêu cầu mức toàn vẹn được quy định của chúng. Do đó, tiêu chuẩn này không quy định cách thức sử dụng mức toàn vẹn tương tác với toàn bộ hệ thống hay các quy trình vòng đời kỹ thuật phần mềm. Tuy nhiên, tiêu chuẩn này đưa ra một ví dụ sử dụng tiêu chuẩn trong Phụ lục B.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là rất cần thiết cho việc áp dụng của 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) Hệ thống và kỹ thuật phần mềm - Đảm bảo phần mềm và hệ thống - Khái niệm và từ vựng

3 Thuật ngữ và định nghĩa

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

CHÚ THÍCH Trong khi một định nghĩa được bao gồm "mức toàn vẹn", các định nghĩa và cộng đồng liên quan hiện thời không đồng tình về định nghĩa "tính toàn vẹn", nhất quán với chính việc sử dụng "mức toàn vẹn". Hơn nữa, không có định nghĩa riêng lẻ nào của "tính toàn vẹn" được đề cập trong tiêu chuẩn này. Định nghĩa "tính toàn vẹn" được sử dụng trong ISO/IEC JTC1 SC7, xem ISO/IEC 25010:2011 *System and software engineering - System and software Quality Requirements and Evaluation (SquaRE) - System and software quality models*.

4 Khung mức toàn vẹn

4.1 Đặc tả mức toàn vẹn

Một đặc tả mức toàn vẹn bao gồm hai loại yêu cầu liên quan, được định nghĩa như sau:

a) **"Mức toàn vẹn"** - một đòi hỏi của một hệ thống, sản phẩm hay phần tử. Đòi hỏi này bao gồm các giới hạn về các giá trị của một đặc tính, phạm vi áp dụng của đòi hỏi và độ không xác định cho phép liên quan tới việc đạt được đòi hỏi. Một nhãn được chỉ định cho một mức toàn vẹn được gọi là nhãn mức toàn vẹn.

b) **"Yêu cầu mức toàn vẹn"** - một tập các yêu cầu được quy định được áp đặt cho các khía cạnh liên quan tới một hệ thống, sản phẩm hay phần tử và các hoạt động liên quan nhằm thể hiện việc đạt được mức toàn vẹn được gán (nhằm đáp ứng đòi hỏi) theo các giới hạn về độ không xác định được yêu cầu. Tập này bao gồm bằng chứng cần để đạt được.

Người định nghĩa mức toàn vẹn cần biện minh rõ ràng sự khẳng định rằng việc đáp ứng các yêu cầu mức toàn vẹn liên quan tới một mức toàn vẹn là đủ để đạt được mức toàn vẹn theo độ không xác định cho phép của nó. Biện minh này có thể được phản ánh, nhưng không cần thiết bao hàm một nguồn cho người dùng (ví dụ: một tiêu chuẩn)

CHÚ THÍCH 1 Mục a) và b) của TCVN 10607-3 đề cập tới "mức toàn vẹn" và "yêu cầu toàn vẹn" một cách tuần tự. Khái niệm "yêu cầu toàn vẹn" đã được thay đổi với "yêu cầu mức toàn vẹn" nhằm tăng cường sự rõ ràng và bởi nó được sử dụng phổ biến trong sự an toàn.

CHÚ THÍCH 2 "Mức toàn vẹn" liên quan tới "đòi hỏi mức toàn vẹn" nhằm phân biệt với "yêu cầu mức toàn vẹn".

CHÚ THÍCH 3 Xem Điều 8.2 và 8.2.4 để có thêm giải thích chi tiết về "giới hạn được yêu cầu".

CHÚ THÍCH 4 Xem TCVN 10607-1 để có nhiều giải thích hơn về việc sử dụng bằng chứng.

CHÚ THÍCH 5 IEEE Std 1012:2004 định nghĩa "mức toàn vẹn" là: "một giá trị đại diện cho các thuộc tính đặc thù của dự án (ví dụ: độ phức tạp phần mềm, độ tới hạn, rủi ro, mức an toàn, công năng mong muốn, độ tin cậy) nhằm xác định tầm quan trọng của một phần mềm cho người dùng". Mức toàn vẹn là một giá trị đặc tính của phần mềm đối tượng. Khi một đòi hỏi và một giá trị có thể coi như đề xuất của một hệ thống hay phần mềm, hai định nghĩa của mức toàn vẹn có cùng một ý nghĩa đáng kể.

CHÚ THÍCH 6 Đòi hỏi mức toàn vẹn trong tiêu chuẩn này có thể bao hàm các hành vi hoặc điều kiện của hệ thống hay sản phẩm hoặc giá trị của một đặc tính, trong trường hợp chúng có thể thực hiện cả hai vai trò: "yêu cầu" và "đo lường". Đối với

một thu thập hệ thống hay sản phẩm, một đòi hỏi mức toàn vẹn có thể sử dụng nhằm thể hiện một thỏa thuận giữa nhà thâu nhận và nhà cung cấp. Trong trường hợp này, đòi hỏi mức toàn vẹn đóng vai trò một yêu cầu. Trong hoạt động chấp nhận một hệ thống hay sản phẩm trong quy trình thu thập, đòi hỏi mức toàn vẹn được sử dụng nhằm xác nhận rằng hệ thống hay sản phẩm được cung cấp theo thỏa thuận, ví dụ: hệ thống hay sản phẩm được cung cấp được cân nhắc bởi một đòi hỏi mức toàn vẹn.

CHÚ THÍCH 7 Mức toàn vẹn và tiêu chuẩn sử dụng mức toàn vẹn này có một lịch sử quan trọng, đặc biệt là trong sự an toàn. Mức toàn vẹn trong các tiêu chuẩn liên quan tới an toàn được định nghĩa như các hệ đa mức, đề cập tới nhiều mức khác nhau của tính chính xác và/hoặc độ không xác định của việc đạt được mức toàn vẹn cho các mức cao hơn dẫn tới tính chính xác hơn và độ không xác định nhỏ hơn. Ví dụ về tiêu chuẩn an toàn là IEC 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems* liên quan tới sự an toàn có thể lập trình. Nói cách khác, những giản đồ tương tự được sử dụng với các nhãn khác nhau, ví dụ: “lớp phù hợp”.

Nhằm hoàn thiện khung mức toàn vẹn, điều tiếp theo mô tả một quy trình sử dụng mức toàn vẹn và cũng đưa ra một nền tảng kiến thức cho nhu cầu và động cơ thúc đẩy được nói đến trong quá trình định nghĩa mức toàn vẹn.

4.2 Quy trình sử dụng mức toàn vẹn

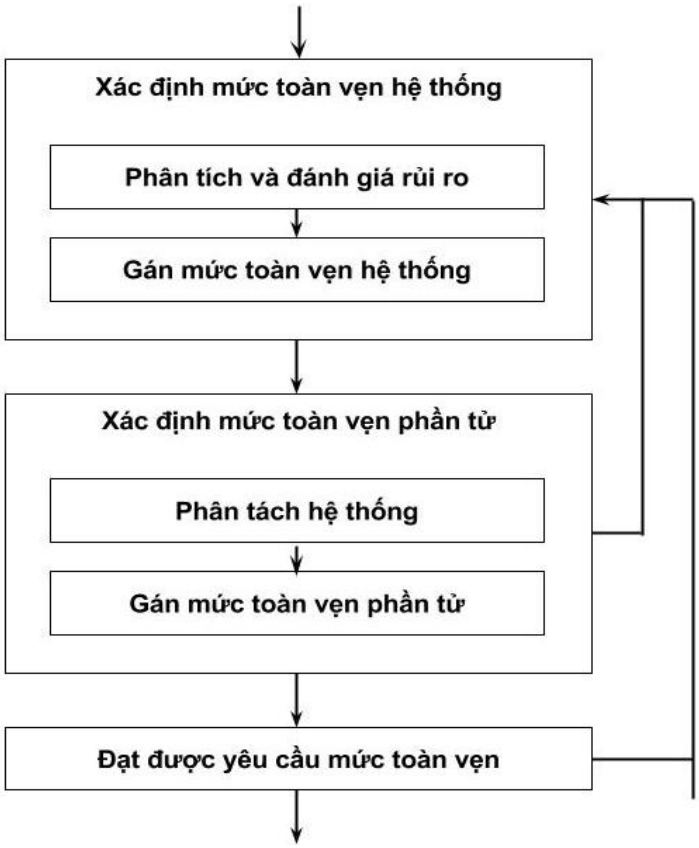
Một cách tiếp cận dựa trên rủi ro được sử dụng trong tiêu chuẩn này nhằm xác định mức toàn vẹn được gán cho hệ thống hay sản phẩm. Theo mức toàn vẹn của hệ thống hay sản phẩm này, mức toàn vẹn được bắt nguồn từ các thành phần hệ thống hay sản phẩm. Hình 1 thể hiện tổng quan các hoạt động được yêu cầu sử dụng mức toàn vẹn. Đầu vào và đầu ra cho mỗi hoạt động được thể hiện tại Bảng A.1, Phụ lục A. Bên cạnh các vòng lặp phản hồi chính được thể hiện trong Hình 1, phản hồi có thể xảy ra giữa tất cả các hành động này.

CHÚ THÍCH 1 ISO/IEC 16085:2006 định nghĩa “rủi ro” là: “sự kết hợp các khả năng xảy ra của một sự kiện và hệ quả của nó”.

Trong tiêu chuẩn này, một hệ thống được coi như có cấu trúc như sau nhằm mở đầu quy trình gán một mức toàn vẹn cho một hệ thống. Đầu tiên, một hệ thống có nhiều giao diện, mỗi giao diện là một ranh giới giữa hệ thống và môi trường của nó. Bất kỳ sự ảnh hưởng nào tới/vào hệ thống được thể hiện bởi khái niệm này, ví dụ: các hoạt động của người dùng, các tương tác với hệ thống khác và các cuộc tấn công bởi người dùng có chủ ý gây hại.

Một hệ thống bao gồm các phần tử hệ thống là các đơn vị tương ứng với một mức toàn vẹn cho các mục đích khác nhau của tiêu chuẩn này. Nhiều cách hiện có nhằm chọn ra các phần tử hệ thống. Việc phân tách một hệ thống thành các phần tử được thực hiện trước hay trong quá trình gán mức toàn vẹn được mô tả trong tiêu chuẩn này. Một phần tử hệ thống có thể được coi như một hệ thống và do đó mối liên hệ hệ thống-phần tử có thể được tìm thấy ở mỗi tầng phân tách hệ thống.

CHÚ THÍCH 2 Một “phần tử hệ thống” đôi khi được nhắc tới như một “phần tử” nếu ngữ cảnh được hiểu đúng.



Hình 1 - Tổng quan các hoạt động cho việc xác định mức toàn vẹn

Nhằm xác định mức toàn vẹn của hệ thống hay sản phẩm, một tính toán tiêu chí rủi ro cho hệ thống mục tiêu được xây dựng nhằm xác định khía cạnh nào (ví dụ: sự kiện, điều kiện của hệ thống, hoàn cảnh môi trường,.v..v.) được xem xét như một rủi ro. Dựa vào các tiêu chí, rủi ro liên quan tới hệ thống hay sản phẩm được phân tích và đánh giá nhằm xây dựng các giới hạn về định thời gian, sự xuất hiện các hệ quả tiêu cực và những điều kiện phát sinh. Các giới hạn này tốt nhất là được xây dựng trước bằng việc giới hạn sự xuất hiện các sự kiện bắt đầu cho những điều kiện này. Một khi các giới hạn này được xây dựngp, các hạn chế về hành vi trong hệ thống hay sản phẩm nhận được mà nếu thỏa mãn sẽ đáp ứng những giới hạn về hệ quả tiêu cực, các điều kiện và sự kiện bắt đầu theo các giới hạn về độ không xác định cho phép.

CHÚ THÍCH 3 Đây là ngữ cảnh phổ biến hơn trong đó mức toàn vẹn được sử dụng, tiêu chuẩn này nói về sự hạn chế tổn thất (ví dụ: hệ quả tiêu cực, các nguy hiểm hay rủi ro) nhưng được áp dụng tương tự nhằm thu được lợi ích.

CHÚ THÍCH 4 Một “hệ quả tiêu cực” là một hệ quả liên kết với một tổn thất.

CHÚ THÍCH 5 Cụm từ “sự kiện bắt đầu” và những khái niệm liên quan được giải thích trong TCVN 10607-1.

Đối với các hệ thống, các hành vi có thể dẫn tới các hệ quả tiêu cực, giới hạn giá trị của các đặc tính phản ánh những giới hạn được yêu cầu theo sự xuất hiện, định thời và/hoặc độ không xác định cho phép liên quan tới những hành vi này. Ví dụ: Đối với các hệ thống, sản phẩm hay các phần tử thực hiện một chức năng giảm thiểu, các đặc tính cần quan tâm bao gồm sự chắc chắn được viện chứng, khả năng áp dụng và độ tin cậy của dịch vụ của chúng.

Nhằm gán một mức toàn vẹn cho một hệ thống, sản phẩm hay phần tử thực tế nhằm gán các mức toàn vẹn cho hệ thống, sản phẩm hay các giao diện phần tử liên quan tới các hệ quả đáng quan tâm. Các hành vi khác nhau của hệ thống hay sản phẩm có thể dẫn tới các mức độ rủi ro nghiêm trọng khác nhau như có thể là các hành vi liên quan tới mỗi giao diện bên ngoài, ví dụ: kết quả của việc phân giới với các thực thể khác. Điều tương tự là đúng cho các giao diện giữa các phần tử hệ thống nội bộ.

CHÚ THÍCH 6 Các mức toàn vẹn khác nhau có thể được gán cho các giao diện khác nhau. Giao diện bên ngoài của một hệ thống hay sản phẩm có thể truy nhập trong ranh giới của nó và được thực hiện bởi hệ thống hay các phần tử sản phẩm. Tương tự, các mức toàn vẹn có thể được gán cho một phần tử hệ thống bên ngoài mà theo đó hệ thống hay sản phẩm phụ thuộc và cơ chế kết nối các phần từ hệ thống bên ngoài.

CHÚ THÍCH 7 Trong tiêu chuẩn này, các phần tử hệ thống bên ngoài mà theo đó hệ thống hay sản phẩm phụ thuộc đôi khi được đề cập một cách ngắn gọn hơn: “phần tử bên ngoài” và được bao gồm khi “phần tử” được đề cập tới, trừ khi được chỉ ra về mặt khác. “Phần tử bên ngoài” bao gồm các dịch vụ bên ngoài, cơ chế kết nối bên ngoài hoặc vận chuyển dịch vụ.

Các mức toàn vẹn cho phần tử bên trong cũng như phần tử bên ngoài mà theo đó (các) mức toàn vẹn hệ thống hay sản phẩm phụ thuộc bắt nguồn từ các mức toàn vẹn được gán cho hệ thống hay các giao diện sản phẩm. Mỗi mức toàn vẹn có một tập yêu cầu mức toàn vẹn tương ứng cần phải thỏa mãn hệ thống, các khía cạnh, hành động cũng như bằng chứng liên quan tương ứng. Bằng chứng này đạt được nhằm biện minh rằng: các mức toàn vẹn được đáp ứng theo độ không xác định cho phép.

5 Sử dụng tiêu chuẩn

5.1 Sử dụng tiêu chuẩn

Mục đích sử dụng của tiêu chuẩn này là định nghĩa một hay một tập các mức toàn vẹn, cách sử dụng các mức toàn vẹn trong suốt vòng đời hệ thống hay sản phẩm, việc gán các mức toàn vẹn cho một hệ thống hay sản phẩm và các phần tử của nó. Các mức toàn vẹn được dùng nhiều nhất trong các quy trình thiết kế, thi hành, xác minh và bảo trì nhằm đảm bảo hệ thống hay sản phẩm có các giá trị đặc tính để giảm thiểu những rủi ro liên quan trong suốt quá trình vận hành, ví dụ: một mức tin cậy nhất định.

CHÚ THÍCH 1 Thuật ngữ “thiết kế” trong tiêu chuẩn này bao gồm các thiết kế từ tất cả hệ thống hay các quy trình vòng đời phần mềm, ví dụ: thiết kế kiến trúc trong ISO/IEC 15288:2008; thiết kế kiến trúc hệ thống, thiết kế kiến trúc phần mềm và thiết kế phần mềm chi tiết trong ISO/IEC 12207:2008.

CHÚ THÍCH 2 Nếu tiêu chuẩn này chỉ được áp dụng với phần mềm, mức toàn vẹn hệ thống và các mức toàn vẹn phần tử phi-phần mềm chỉ được yêu cầu nhằm xác định các mức toàn vẹn phần tử phần mềm.

Mặc dù định nghĩa, cách xác định và áp dụng mức toàn vẹn được thực hiện trong ngữ cảnh áp dụng quản lý rủi ro, tiêu chuẩn này bao hàm việc phân tích và đánh giá rủi ro mức cao và không bao hàm các phân tích rủi ro kỹ thuật và chuyên ngành. Các thông tin bổ sung cần thiết nhằm bổ sung cho các yêu cầu mức cao theo các phân tích rủi ro được bao gồm trong tiêu chuẩn này và có thể được tìm thấy tại các điều khoản trong Thư mục tài liệu viện dẫn.

Người dùng tiêu chuẩn này cần đọc tất cả các điều do việc hiểu định nghĩa mức toàn vẹn và cách sử dụng mức toàn vẹn yêu cầu sự hiểu biết mang tính tương hỗ. Các khía cạnh trong việc định nghĩa mức toàn vẹn chỉ ra cách sử dụng và nhu cầu của người dùng. Biết được cách sử dụng có thể giúp cho việc làm rõ các động cơ thúc đẩy cho việc xác định các mức toàn vẹn và tạo ra các sản phẩm công việc. Hiểu biết các yêu cầu cho cách sử dụng các mức toàn vẹn yêu cầu hiểu biết định nghĩa của chúng.

Tiêu chuẩn này có thể được sử dụng riêng hoặc kết hợp với các tiêu chuẩn khác của bộ TCVN 10607. Tiêu chuẩn này có thể được sử dụng với một loạt các phân tích rủi ro chuyên ngành, kỹ thuật và các cách tiếp cận phát triển được tham chiếu trong TCVN 10607-1. TCVN 10607-1 đưa ra các thông tin bổ sung và tài liệu tham khảo nhằm hỗ trợ người dùng tiêu chuẩn này.

Các trường hợp đảm bảo được bao hàm bởi TCVN 10607-2. TCVN 10607-2 không yêu cầu cách sử dụng trường hợp đảm bảo nhưng mô tả cách thức mức toàn vẹn và trường hợp đảm bảo có thể cùng làm việc, đặc biệt là trong định nghĩa các đặc tả cho mức toàn vẹn hoặc thông qua việc sử dụng mức toàn vẹn trong một phần của trường hợp đảm bảo.

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

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

5.2 Tài liệu

Các kết quả, tạo tác và công năng của các hoạt động được bao trùm bởi tiêu chuẩn này phải được văn bản hóa và đảm bảo tính toàn vẹn của tài liệu. Các yêu cầu cho tài liệu dự kiến, các thỏa thuận và phê duyệt thực tế được đề cập trong Điều 11.4.

5.3 Nhân viên và tổ chức

Nhân viên và tổ chức thực hiện các hành động được bao trùm trong tiêu chuẩn này phải có đủ khả năng, và các tổ chức phải quan tâm một cách hợp lý về mục đích và niềm tin của nhân viên. Các tổ chức cần đảm bảo những yêu cầu này được đáp ứng bằng cách thực hiện các hành động liên quan tới tính nghiêm trọng của các rủi ro liên quan và tuân theo bất kỳ yêu cầu chỉ đạo nào. Bằng chứng về khả năng có thể là một phần của trường hợp đảm bảo.

5.4 Tổng quan về tiêu chuẩn

Điều 5, 5.4 và 11 liên quan tới định nghĩa mức toàn vẹn. Điều 5, 7, 8, 9, 10 và 11 liên quan tới cách sử dụng mức toàn vẹn. Mục đích và kết quả cho việc sử dụng tiêu chuẩn này được đề cập tại Điều 6.1 và

6.2 cho việc định nghĩa mức toàn vẹn; tại Điều 7.1 và 7.2 cho việc sử dụng các mức toàn vẹn. Những điều kiện tiên quyết cho việc định nghĩa và sử dụng mức toàn vẹn được bao trùm lần lượt trong Điều 6.3 và 7.3. Các thẩm quyền được xác định, các thỏa thuận và phê duyệt được bao trùm trong Điều 11. Phụ lục A bao gồm các đầu vào và đầu ra cho khung mức toàn vẹn được minh họa trong Hình 1. Phụ lục B đưa ra một ví dụ lý thuyết bao trùm các khía cạnh của các Điều 5.4, 7, 8 và 9.

6 Định nghĩa mức toàn vẹn

6.1 Mục đích của việc sử dụng tiêu chuẩn

Một tập mức toàn vẹn được xác định cho việc sử dụng trong một phạm vi áp dụng nhất định nhằm gán các mức toàn vẹn cho một hệ thống hay sản phẩm, các phần tử bên trong và bên ngoài mà đòi hỏi hệ thống hay sản phẩm phụ thuộc. Mỗi mức toàn vẹn có các yêu cầu mức toàn vẹn tương ứng mà nếu đáp ứng sẽ thể hiện việc đạt được đòi hỏi mức toàn vẹn cho hệ thống, sản phẩm hay phần tử trong độ không xác định cho phép. Đưa ra một tập các mức toàn vẹn được sử dụng phù hợp và việc đòi hỏi mức toàn vẹn liên quan tới các hành vi của hệ thống hay sản phẩm là đúng đắn, các rủi ro tương ứng được hạn chế hay được quản lý theo một cách chấp nhận được.

6.2 Kết quả của việc sử dụng tiêu chuẩn

Nhằm thể hiện sự phù hợp với tiêu chuẩn này, tài liệu hiện hành phải chính xác và khả dụng, ví dụ: được yêu cầu, kiểm soát, có thể truy xuất và đánh giá mà tính toàn vẹn được bảo toàn; và bao gồm những điều sau:

a) Một phân tích thể hiện sự phù hợp của một tập thứ bậc các mức toàn vẹn trong phạm vi áp dụng nhất định của nó.
b) Đối với mỗi mức toàn vẹn được xác định rõ ràng:
    1) Chỉ định đòi hỏi của mức toàn vẹn, ví dụ: các hạn chế về giá trị đặc tính, phạm vi áp dụng và độ không xác định cho phép của sự đạt được.
    2) Biện minh rằng:
        i. Đáp ứng các yêu cầu mức toàn vẹn thể hiện sự đạt được đòi hỏi theo độ không xác định cho phép.
        ii. Đạt được bằng chứng được yêu cầu thể hiện việc đáp ứng yêu cầu mức toàn vẹn theo độ không xác định cho phép.
c) Các đặc tả, yêu cầu có thể sử dụng và hướng dẫn rõ ràng cho việc đảm bảo việc sử dụng tập mức toàn vẹn phù hợp theo phạm vi áp dụng của nó. Cách sử dụng đó bao gồm các hành động được thực hiện liên quan tới độ không xác định và các kết quả tương ứng, sự phân bổ ban đầu của mức toàn vẹn hệ thống hay sản phẩm và sự phẩn bổ các mức toàn vẹn cho phần tử hệ thống.
d) Việc xác định bên phê duyệt cho định nghĩa mức toàn vẹn và các kết quả thỏa thuận và hoạt động phê duyệt cho các thỏa thuận trước đây và hiện có.
e) Các biên bản thể hiện sự phù hợp với các yêu cầu quy định của tiêu chuẩn này, cho việc định nghĩa các mức toàn vẹn được bao gồm trong Điều 5.4.
f) Các sản phẩm công việc liên quan bao gồm lịch sử và sơ cứ có thể được duy trì và soát xét nếu cần.

6.3 Điều kiện tiên quyết cho việc định nghĩa mức toàn vẹn

6.3.1 Xác lập lĩnh vực phù hợp cho việc sử dụng mức toàn vẹn

6.3.1.1 Tổng quan

Không phải tất cả lĩnh vực đều phù hợp với việc định nghĩa và sử dụng mức toàn vẹn. Mức toàn vẹn phải được định nghĩa cho một lĩnh vực chỉ khi một phần kinh nghiệm liên quan quan trọng tồn tại cho lĩnh vực được hiểu rõ bởi việc thực hiện định nghĩa đó.

6.3.1.2 Rủi ro

Các thông tin sau đây về các rủi ro phải được hiểu rõ theo một phần kinh nghiệm liên quan quan trọng:

a) Những quan tâm liên quan tới rủi ro - hệ quả tiêu cực tiềm ẩn, sự xuất hiện cũng như những tiền đề của chúng.
b) Đặc tính đáng quan tâm (có thể là đặc tính tổng hợp) và những giới hạn về giá trị của đặc tính (thông qua các mức rủi ro được phép và mức toàn vẹn tương ứng)
c) Các giới hạn được yêu cầu về độ không xác định bao gồm các mức rủi ro cho phép và tập mức toàn vẹn.

CHÚ THÍCH Trong toàn bộ tiêu chuẩn này, việc sử dụng từ “cho phép” được hiểu là bao gồm “chấp nhận được” và “có thể chịu được”. Tương tự, “không cho phép” bao gồm “không chấp nhận được” và “không chịu được”.

6.3.1.3 Môi trường của hệ thống hay sản phẩm

Những thông tin sau đây về môi trường của hệ thống hay sản phẩm phải được hiểu rõ trong một phần kinh nghiệm liên quan quang trọng:

a) Các điều kiện và hoạt động, trong đó hệ thống hay sản phẩm được bao gồm (thông qua phần liên quan của vòng đời)
b) Các hạn chế trong việc vận hành và bảo trì hệ thống hay sản phẩm.
c) Cấu trúc phụ thuộc của hệ thống hay sản phẩm, bao gồm các phần tử và tương tác với môi trường
d) Các phương pháp thiết kế, thực hiện, kiểm tra và đánh giá, chuyển tiếp, vận hành, bảo trì và chuyển nhượng.
e) Các hành vi liên quan tới môi trường, bao gồm các ảnh hưởng tới hệ thống và tương tác giữa các phần tử hệ thống.

6.3.1.4 Bằng chứng liên quan

Một phần bằng chứng quan trọng nên sẵn có để độ không xác định tồn tại vừa đủ thấp cho việc định nghĩa dựa trên bằng chứng được thực hiện. Kiến thức liên quan tới các tình huống bình thường hay bất thường đều cần tồn tại trong phạm vi áp dụng và môi trường trung gian hay môi trường liên quan khác.

CHÚ THÍCH Khi dựa vào bằng chứng cũ, một định nghĩa nên thỏa mãn mục đích sử dụng dự kiến.

6.3.2 Xác lập mục đích và phạm vi sơ bộ

Mục đích dự kiến và phạm vi sơ bộ cho mức toàn vẹn phải được xác lập nhằm đảm bảo sự tham gia của các cá nhân, tổ chức, chuyên gia và trải nghiệm cần thiết.

6.4 Sự nhất quán với yêu cầu sử dụng

Tất cả các phần của định nghĩa một hay một tập mức toàn vẹn phải được nhất quán với các yêu cầu của việc sử dụng mức toàn vẹn, được bao trùm tại Điều 5, 7, 8, 9, 10 và 11. Bất kỳ tài liệu nào đi kèm mà không đáp ứng các yêu cầu này cần đưa ra biện minh bằng văn bản và được gán nhãn rõ ràng nếu tồn tại cách khác. Các thỏa thuận và phê duyệt liên quan đạt được dựa theo Điều 11.

6.5 Phân tích phạm vi áp dụng

Lợi ích từ các mức toàn vẹn là dựa trên một phần của khả năng áp dụng được phép bởi đặc tính tổng quát của các mức toàn vẹn. Phạm vi áp dụng dựa trên đặc tính tổng quát của biện minh về các yêu cầu mức toàn vẹn tương ứng.

Biện minh này ngược lại là kết quả từ một hiểu biết thấu đáo phạm vi áp dụng và phân tích đi kèm. Phân tích được thực hiện nhằm tạo ra các đặc tả mức toàn vẹn và đảm bảo khả năng áp dụng, sự phù hợp, sự chuẩn xác, sự hoàn thiện cần thiết và độ không xác định cho phép của mức toàn vẹn liên quan tới việc sử dụng mức toàn vẹn. Biện minh này bao gồm việc chỉ ra các khía cạnh được liệt kê trong Điều 6.3.1.

Bất kỳ phân tích rủi ro nào cần phù hợp với các yêu cầu của Điều 8.2.3 Các phân tích rủi ro.

CHÚ THÍCH Sử dụng mức toàn vẹn góp phần tạo ra các nền tảng cho niềm tin cậy vào bên liên quan và những hạn chế về độ không xác định. Tuy nhiên, tiêu chuẩn này không làm rõ các yêu cầu cần đáp ứng nhằm đạt được các nền tảng cho mức độ tin tưởng đã chỉ ra hay những hạn chế cụ thể về độ không xác định.

6.6 Ba sản phẩm công việc được yêu cầu

Mức toàn vẹn thường được xác định một lần và sử dụng nhiều lần. Như đã giải thích trong Điều 4.1, các đặc tả mức toàn vẹn bao gồm hai loại yêu cầu và biện minh liên quan tới hai yêu cầu này. Do vậy, ba sản phẩm công việc rõ ràng phù hợp theo khung tại Điều 4.1 phải được văn bản hóa cho mỗi mức toàn vẹn.

a) “Mức toàn vẹn” - Điều mà mức toàn vẹn đạt được hay đòi hỏi: được đặt là một yêu cầu hay đòi hỏi mà hệ thống, sản phẩm hay thành phần đáp ứng:
   1) Một dải giá trị mục tiêu cho một đặc tính, ví dụ: một thuộc tính chất lượng như sự tin cậy hay sự xuất hiện các lỗi nghiêm trọng.
   2) Một giới hạn về khả năng áp dụng - điển hình trong một phạm vi xác định theo những điều kiện cụ thể
   3) Những hạn chế nhất định về độ không xác định.
b) “Yêu cầu mức toàn vẹn” - Điều mà mức toàn vẹn được gán cho:
   1) Điều được thực hiện và cách thức, thời điểm, ví dụ: bao gồm các yêu cầu liên quan tới tổ chức, các quy trình, hoạt động, tác vụ, cách thức, phương tiện và tài nguyên bao gồm nhân

viên và các công cụ, môi trường làm việc, sự giao tiếp, quản lý hay kết hợp, lưu giữ ghi chép và những khía cạnh khác của công năng.

2) Hệ thống, sản phẩm hay thành phần, bao gồm các yêu cầu về tài liệu, dịch vụ và các tạo tác, gồm bất kỳ một phần mềm nào.
3) Bằng chứng có được, có thể bao gồm các hạn chế về độ không xác định cho phép còn lại liên quan tới bằng chứng, ví dụ: độ không xác định còn lại sau khi vượt qua một thử nghiệm.

c) Biện minh "yêu cầu mức toàn vẹn" - Một biện minh thể hiện rằng việc đáp ứng các yêu cầu mức toàn vẹn hỗ trợ cho việc thỏa mãn các yêu cầu mức toàn vẹn theo những hạn chế về độ không xác định cần thiết.

Ba điều sau đây giải thích rõ hơn về những sản phẩm công việc này.

6.6.1 Quy định đòi hỏi mức toàn vẹn

Quy định một đòi hỏi mức toàn vẹn là thiết yếu trong việc xác định ý nghĩa của nó và cần rõ ràng.

Nhằm đảm bảo tầm ảnh hưởng của các điều kiện của việc sử dụng, phạm vi áp dụng của một mức toàn vẹn phải bao gồm sự hiện diện tiềm năng của hệ thống, sản phẩm hay phần tử của:

a) Lỗi ngẫu nhiên, hành vi nguy hiểm và sự kiện.
b) Lỗi có hệ thống trừ khi biện minh bằng văn bản đã được cung cấp để làm điều gì khác.
c) Lỗi, sự kiện và hành vi nguy hiểm dẫn tới sự nguy hại, bao gồm việc xử lý các lỗi này như lỗi có hệ thống, trừ khi biện minh bằng văn bản đã được cung cấp đẻ làm điều gi khác.

6.6.2 Quy định yêu cầu mức toàn vẹn

Việc đáp ứng yêu cầu mức toàn vẹn thể hiện việc đạt được những hạn chế về giá trị của một đặc tính, theo những điều kiện nhất định và một độ không xác định cụ thể.

Bằng chứng được yêu cầu theo các yêu cầu mức toàn vẹn tương ứng của mỗi mức toàn vẹn là thiết yếu nhằm xác định, quy định các yêu cầu mức toàn vẹn và đánh giá việc đạt được của chúng. Nhằm có một sự đặc tả được xác lập một cách chấp nhận được, các yêu cầu mức toàn vẹn phải:

a) Phù hợp với việc biện minh hoặc nguồn gốc liên quan tới mức toàn vẹn theo những yêu cầu mức toàn vẹn của nó (Điều 6.6.3). Những yêu cầu này bao gồm việc bảo đảm sử dụng mức toàn vẹn theo phạm vi áp dụng được hỗ trợ bởi sự biện minh, bao gồm sự phụ thuộc và phương pháp gán các mức toàn vẹn cho hệ thống hay phần tử sản phẩm.
b) Yêu cầu bằng chứng được ấn định bởi các yêu cầu mức toàn vẹn nhằm thể hiện việc đáp ứng tất cả yêu cầu mức toàn vẹn, bao gồm việc đạt được bất kỳ hạn chế nào về độ không xác định.

CHÚ THÍCH 1 Trong một vài tình huống, biện minh của người dùng có thể cần sự diễn giải và áp dụng các yêu cầu mức toàn vẹn (đặc biệt nếu việc lựa chọn giữa các thay thế khả thi) và bằng chứng thể hiện việc đáp ứng các yêu cầu mức toàn vẹn. Biện minh cũng liên quan tới Điều 6.8 Thông tin cung cấp cho người dùng.

c) Bao gồm những khía cạnh liên quan của các thuộc tính và hành vi của hạ tầng theo việc đạt được đòi hỏi dựa trên sự bao gồm bất kỳ cơ chế nào thực hiện một kết nối với các phần tử (hoặc các thực thể) bên ngoài.

d) Bao gồm sự tương tác của các phần tử phụ thuộc trong một hệ thống, sản phẩm hay phần tử nhất quán với việc đạt được mức toàn vẹn của hệ thống, sản phẩm hay phần tử cao hơn.
e) Bao gồm phạm vi được yêu cầu của việc gán các mức toàn vẹn cho các phần tử hệ thống nội bộ và các phần tử khác dựa vào đó.
f) Kéo dài qua thời gian, bao gồm việc theo dõi công năng của hệ thống, sản phẩm hay phần tử nhằm phát hiện và tránh việc vượ qua những hạn chế được yêu cầu nếu có thể thực hiện được.

CHÚ THÍCH 2 Trước khi chuyển tiếp và vận hành, các yêu cầu này có thể được đáp ứng bởi hệ thống hay sản phẩm đưa ra hỗ trợ cần thiết và được bao gồm trong tài liệu, đào tạo, giao diện người dùng, hỗ trợ khác, các thử nghiệm và thỏa thuận nếu được bảo đảm. Khoảng thời gian này thường bao gồm trong quá trình phát triển.

g) Yêu cầu việc đáp ứng các yêu cầu tại Điều 10.
h) Thể hiện tính chính xác, xuyên suốt, chặt chẽ và các thuộc tính chất lượng đực yêu cầu khác của bằng chứng và thông tin đi kèm phù hợp với các yêu cầu được bắt nguồn việc biện minh các yêu cầu mức toàn vẹn.

Việc sử dụng các cách thức thay thế cho việc đáp ứng các yêu cầu mức toàn vẹn được bao quát tại Điều 10.2. Tuy nhiên, các yêu cầu mức toàn vẹn có thể ngăn cấm hay giới hạn các cách thức thay thế. Các yêu cầu mức toàn vẹn nên bao gồm cả việc phát hiện các cảnh báo và chỉ báo của sự cần thiết cho hành động xuyên suốt vòng đời.

6.6.3 Biện minh sự phù hợp giữa đòi hỏi mức toàn vẹn và yêu cầu mức toàn vẹn

6.6.3.1 Tổng quan

Đối với mỗi mức toàn vẹn, biện minh bằng văn bản phải đưa ra, hoặc một hay nhiều nguồn phải được xác định và được biện minh nhằm thể hiện - trong suốt phạm vi áp dụng và theo những hạn chế được yêu cầu về độ không xác định - mà:

a) Đáp ứng các yêu cầu mức toàn vẹn thể hiện sự đạt được đòi hỏi mức toàn vẹn.
b) Đáp ứng các yêu cầu cho bằng chứng thể hiện việc đáp ứng các yêu cầu mức toàn vẹn.

Biện minh bằng văn bản bao gồm tầm ảnh hưởng tới tất cả thực thể mà việc đạt được mức toàn vẹn phụ thuộc. Tài liệu được thỏa thuận và phê duyệt tương ứng với Điều 11.

CHÚ THÍCH 1 Một biện minh riêng lẻ có thể thể hiện rằng việc đáp ứng các yêu cầu cho bằng chứng thể hiện sự đạt được đòi hỏi.

CHÚ THÍCH 2 Các giới hạn và giả định được bao gồm hay ám chỉ qua việc biện minh các yêu cầu mức toàn vẹn là nhất quán với phạm vi áp dụng của mức toàn vẹn. Việc biện minh bao gồm các yêu cầu kỹ thuật được hoàn thiện trong suốt quá trình sử dụng mức toàn vẹn (Điều 6.8), ví dụ: những giới hạn thiết kế và hạn chế phương pháp sử dụng nhằm gán các mức toàn vẹn cho các phần tử hệ thống và phụ thuộc bên ngoài.

6.6.3.2 Sử dụng trường hợp đảm bảo trong biện minh

Một trường hợp bảo đảm có thể được sử dụng trong việc biện minh này. Một vài giới hạn có thể phát sinh từ bản chất của lập luận, đặc biệt là những hạn chế kỹ thuật như phương pháp gán các mức toàn vẹn cho hệ thống trong quá trình thiết kế. Trường hợp đảm bảo tạo ra bằng chứng được yêu cầu. Cấu

trúc của một trường hợp đảm bảo tổng quát có thể bao trùm một hay nhiều mức toàn vẹn. Vì thế, khi một trường hợp đảm bảo được sử dụng, việc đạt được mức toàn vẹn cân bằng với một đòi hỏi trong trường hợp đảm bảo và các yêu cầu mức toàn vẹn của nó được rút ra theo sự cần thiết đảm bảo phạm vi của lập luận, sự nhất quán của các đòi hỏi bên trong noó và việc đạt được bằng chứng được yêu cầu bởi trường hợp đảm bảo.

Việc đảm bảo khả năng áp dụng của lập luận cần bao quát sự bảo đảm phù hợp với các đòi hỏi mức toàn vẹn và điều kiện áp dụng cho các đòi hỏi đó cũng như bất kỳ yêu cầu nào nhằm bảo đảm các giả định. Yêu cầu này bao gồm bất kỳ giới hạn nào về phạm vi của sự phụ thuộc và các phương pháp gán mức toàn vẹn choi hệ thống hay phần tử sản phẩm mà được bao gồm trong việc biện minh.

Các yêu cầu mức toàn vẹn cần bao gồm một tập bằng chứng được yêu cầu của tất cả hay một phần trường hợp đảm bảo (hay tập trường hợp đảm bảo) cũng như bằng chứng mà điều kiện phù hợp giữa đòi hỏi và bất kỳ giả định nào khác của nó được đáp ứng.

CHÚ THÍCH 1 Ví dụ: một cách tiếp cập có thể dưới dạng một trường hợp đảm bảo tổng quát cho lĩnh vực áp dụng và các cách tiếp cận thông thường cho việc thiết kế, thực hiện, vận hành, bảo trì và chuyển nhượng. Cách tiếp cận có thể có đòi hỏi mức cao tương ứng với một đặc tính có tầm quan trọng rộng lớn (ví dụ: sự an toàn), các giới hạn hữu dụng về giá trị đặc tính và độ không xác định theo những điều kiện cụ thể và một lập luận mà bao gồm sự cần thiết của lĩnh vực áp dụng.

CHÚ THÍCH 2 Một vài ý niệm về mức toàn vẹn, bao gồm các biện minh yêu cầu mức toàn vẹn và bằng chứng của nó, tương tự với mục đích của một trường hợp bảo đảm tổng quát, tiền đóng gói và có thể tái sử dụng. Ngược lại, các mức toàn vẹn có thể được sử dụng nhằm hỗ trợ một đòi hỏi trong trường hợp bảo đảm khi đòi hỏi phù hợp một mức toàn vẹn.

6.7 Duy trì đặc tả mức toàn vẹn

Việc duy trì sự hữu dụng và lợi ích của đòi hỏi mức toàn vẹn, các yêu cầu mức toàn vẹn tương ứng, sự hiệu lực và thích hợp của biện minh thỏa mãn các đặc tính tính này là động cơ thúc đẩy chính cho việc cập nhật đặc tả mức toàn vẹn và biện minh liên quan. Đặc tả mức toàn vẹn và biện minh liên quan phải được duy trì, bao gồm việc đánh giá sự cần thiết có thể đối việc cập nhật bất kỳ lúc nào một thay đổi quan trọng tiềm ẩn xảy ra hoặc một bỏ sót trước đó được khám phá trong lĩnh vực áp dụng của mức toàn vẹn. Một thay đổi quan trọng bao gồm các nhân tố mới được khám phá hoặc đang bị làm xấu đi (ví dụ: các nhân tố hay hệ quả tiêu cực của chúng trở nên lớn hơn, thường xuyên hơn, nhiều khả năng xảy ra hơn, lâu hơn, khó đoán trước hơn, sớm hơn dự tính hay tốn nhiều chi phí hơn) như những nhân tố sau đây:

a) Chiều rủi ro với quan hệ quan trọng tiềm ẩn.
b) Điều kiện nguy hiểm.
c) Sự kiện bắt đầu.
d) Nguồn nguy hiểm.
e) Nguồn hay mức độ không xác định.
f) Hệ quả.
g) Sự thiếu hụt năng lực.
h) Cơ chế giảm thiểu.
i) Giao diện, tương tác, kết nối hay phụ thuộc của một hệ thống áp dụng với môi trường của nó

CHÚ THÍCH "Điều kiện nguy hiểm" được giải thích rõ hơn tại Điều 8 và trong TCVN 10607-1.

6.8 Thông tin cung cấp cho người dùng

6.8.1 Yêu cầu

Các đặc tả cho các mức toàn vẹn phải bao gồm hoặc được đi kèm bởi thông tin cho phép người dùng:

a) Hiểu về tập mức toàn vẹn và các yêu cầu mức toàn vẹn tương ứng.
b) Xác lập phạm vi áp dụng của một mức (hay tập) mức toàn vẹn bao gồm phạm vi sử dụng.
c) Xem xét tính khả thi và khả năng sử dụng..
d) Thực hiện hoạt động tuân theo các biện minh mức toàn vẹn, cụ thể là trong việc gán mức toàn vẹn cho các hệ thống, sản phẩm và phần tử. Từ (các) mức toàn vẹn được gán cho một hệ thống hay sản phẩm, các hoạt động vi này chuyển hóa các mức toàn vẹn được gán cho các phần tử hệ thống và phần tử bên ngoài mà nó dựa vào.
e) Xác lập xem liệu yêu cầu mức toàn vẹn đã được đáp ứng.
f) Thực hiện các hoạt động và/hoặc sử dụng các phương pháp liên quan tới độ không xác định tương ứng.
g) Xác định bên phê duyệt cho đặc tả mức toàn vẹn, bao gồm việc biện minh, các tài liệu và hỗ trợ đi kèm.

6.8.2 Hướng dẫn và khuyến nghị

Thông tin nên được cung cấp nhằm hỗ trợ người dùng mức toàn vẹn, bao gồm

a) Sự thấu hiểu và hỗ trợ liên quan tới phân tích rủi ro và đánh giá mức độ thực tế.
b) Hướng dẫn về việc xác định mức toàn vẹn nhằm gán cho một hệ thống hay sản phẩm - ví dụ: các tình huống mà gán một mức toàn vẹn cụ thể cho một giao diện bên ngoài đặc biệt của hệ thống hay sản phẩm.
c) Thông tin nhằm tạo điều kiện kỹ thuật nhất quán với việc biện minh các yêu cầu mức toàn vẹn.
d) Hướng dẫn nhằm tạo điều kiện cho việc đáp ứng các yêu cầu tại Điều 10.

7 Sử dụng mức toàn vẹn

7.1 Mục đích sử dụng tiêu chuẩn

Một mức toàn vẹn được gán cho một dịch vụ hay sản phẩm chỉ ra một đòi hỏi tương ứng với các hành vi và điều kiện của hệ thống hay sản phẩm đó, mục tiêu sử dụng các mức toàn vẹn được đáp ứng nếu đòi hỏi này là đúng. Nói chung, mục tiêu này nên hạn chế hoặc quản lý các rủi ro tương ứng với hệ thống hay sản phẩm có khả năng chấp nhận. Mức toàn vẹn thu được cho mỗi phần tử hệ thống chỉ ra một đòi hỏi liên quan tới các hành vi đó theo đòi hỏi mức toàn vẹn của hệ thống hay sản phẩm mà nó phụ thuộc. Mỗi mức toàn vẹn được gán có các yêu cầu mức toàn vẹn mà khi đáp ứng việc thể hiện đạt được đòi hỏi mức toàn vẹn của phần tử hệ thống với độ không xác định cho phép.

CHÚ THÍCH Việc sử dụng các mức toàn vẹn thường góp phần tạo ra các nền tảng cho niềm tin của bên liên quan và hỗ trợ cho việc đưa ra quyết định của họ.

7.2 Kết quả sử dụng tiêu chuẩn

Nhằm thể hiện sự phù hợp với tiêu chuẩn này cho việc sử dụng mức toàn vẹn, tài liệu hiện thời phải chính xác, sẵn có khi được yêu cầu, được kiểm soát, có khả năng truy xuất, đánh giá, tính toàn vẹn được đảm bảo; và bao gồm các điều sau:

a) Đòi hỏi mức toàn vẹn, ví dụ: các giới hạn giá trị đặc tính, điều kiện áp dụng và các giới hạn về độ không xác định.
b) Các yêu cầu mức toàn vẹn cho mỗi mức toàn vẹn được sử dụng.
c) Việc biện minh hay nguồn mà:
    1) Đáp ứng các yêu cầu mức toàn vẹn tương ứng đủ để thể hiện việc đạt được đòi hỏi mức toàn vẹn.
    2) Bao gồm bằng chứng cần thiết nhằm thể hiện việc đáp ứng các yêu cầu mức toàn vẹn.

CHÚ THÍCH Các kết quả a) và b) phải được rút ra từ việc định nghĩa mức toàn vẹn (xem Điều 5.4). Trong khi tiêu chuẩn này có thể được sử dụng với các mức toàn vẹn mà không được định nghĩa theo sự phù hợp với Điều 6 mục a), b) và c) là luôn được yêu cầu.

d) Việc định danh duy nhất bao gồm phiên bản, ngày tháng, con số, một hay nhiều trường hợp và thẻ thông tin cho một hệ thống, sản phẩm hay phần tử mà sự phù hợp được đòi hỏi.
e) Việc gán một mức toàn vẹn cho hệ thống hay sản phẩm.
f) Các phép gán mức toàn vẹn cho các phần tử hệ thống theo hệ thống hay sản phẩm dựa trên việc đạt được của một hay một tập mức toàn vẹn hệ thống hay sản phẩm được gán và việc biện minh của phép gán đó cho các phần tử hệ thống.
g) Các hoạt động được thực hiện liên quan tới độ không xác định và kết quả tương ứng của chúng.
h) Trình độ chuyên môn của phương pháp và công cụ được sử dụng và các biện minh sử dụng chúng.
i) Bằng chứng cần thiết với các yêu cầu mức toàn vẹn của mức toàn vẹn được gán, hay việc thể hiện việc đạt được mức toàn vẹn có thể chấp nhận được, hoặc các yêu cầu mức toàn vẹn theo các cách thức xác minh khác. Bằng chứng thu được là chính xác, tính toàn vẹn được đảm bảo, tính sẵn có cần thiết của nó được nêu ra.
j) Các kết quả của thỏa thuận hiện tại và bất kỳ hoạt động xác minh nào trước đó.
k) Các biên bản thể hiện sự phù hợp với các yêu cầu viện dẫn của tiêu chuẩn này liên quan tới việc sử dụng mức toàn vẹn.
l) Các sản phẩm công việc liên quan có thể thừa nhận việc đáp ứng các yêu cầu mức toàn vẹn được gán.

7.3 Điều kiện tiên quyết cho việc sử dụng mức toàn vẹn

7.3.1 Xác định phạm vi của rủi ro được bao trùm

Việc xác định phạm vi của tiêu chuẩn này được áp dụng phải phản ánh đúng các bên liên quan và sự quan tâm của họ. Việc xác định cũng phải phản ánh các quyết định trước khi chỉ ra một phạm vi cho các rủi ro được bao trùm theo tiêu chuẩn này và phạm vi của các rủi ro được bao trùm ở nơi khác. Việc

phân bổ này có thể được hoàn thiện bởi các chiều rủi ro (ví dụ: an toàn, kinh tế, an ninh) hoặc điều khác. Các điều sau được áp dụng:

a) Kết quả của việc quyết định phạm vi phải được định nghĩa rõ ràng, được đồng ý và thừa nhận dựa trên Điều 11 và được văn bản hóa.
b) Phạm vi bao trùm theo tiêu chuẩn này phải tương ứng với việc đạt được mục đích sử dụng dự kiến.
c) Phạm vi phải bao trùm tính nguy hại trừ khi một biện minh nhạy cảm được văn bản hóa, được đồng ý và thừa nhận dựa trên Điều 11.
d) Tất cả hệ quả tiêu cực và rủi ro liên quan tới hệ thống hay sản phẩm cần được xác định là khả năng phản hồi được gán ở đâu đó - ở bên trong hay bên ngoài phạm vi của các hoạt động được bao trùm bởi tiêu chuẩn này.
e) Bất kỳ khi nào các rủi ro hay các điều kiện khác liên quan được khám phá mà không ai có khả năng phản hồi để phân tích, các rủi ro đó phải được gán cho các cá nhân và/hoặc tổ chức liên quan và phải được xác định cho việc thỏa thuận và bên phê duyệt dựa trên Điều 11.

7.3.2 Xác lập khả năng áp dụng mức toàn vẹn cho phạm vi sử dụng

Một hay một tập mức toàn vẹn được sử dụng từ một hay nhiều nguồn xác định phải được áp dụng cho tình huống mà sản phẩm hay hệ thống, trong đó một hay một tập mức toàn vẹn được gán, bao gồm khả năng áp dụng cho mỗi:

a) Đòi hỏi mức toàn vẹn.

b) Yêu cầu mức toàn vẹn.

c) Biện minh của các yêu cầu mức toàn vẹn xác lập hỗ trợ cho đòi hỏi. Biện minh này bao gồm các phụ thuộc và phương pháp gán mức toàn vẹn cho hệ thống hay các phần tử sản phẩm được bao gồm trong biện minh.

Phạm vi, bản chất và các giới hạn của tất cả mức toàn vẹn này yêu cầu khả năng áp dụng theo tình huống, hệ thống hay sản phẩm, bao gồm các lập luận, giả định và bằng chứng được sử dụng trong việc biện minh. Hơn nữa, các tài liệu đi kèm mức toàn vẹn phải phù hợp với phạm vi sử dụng dự kiến.

7.3.3 Quyết định vai trò của mức toàn vẹn trong vòng đời

Người dùng tiêu chuẩn này phải xác lập vai trò dự kiến của các mức toàn vẹn trong hệ thống hay vòng đời sản phẩm. Quy trình được mô tả trong tiêu chuẩn này được trình bày như sự khác biệt so với toàn bộ quy trình vòng đời. Mục đích của tiêu chuẩn này nhằm khuyến khích chứ không yêu cầu việc sử dụng mức toàn vẹn được tương tác với các quy trình vòng đời sản phẩm hay phần mềm.

7.3.4 Xác lập cách tiếp cận cho việc phân tích rủi ro

Cách tiếp cận với việc phân tích và đánh giá rủi ro cần phù hợp theo tình huống. Việc phân tích rủi ro có thể được thực hiện cho các lý do khác sẵn có, việc phân tích này được tăng cường khi cần thiết. Các tiêu chuẩn hay hướng dẫn có thể tồn tại cho việc sử dụng trong một phạm vi liên quan. Hơn nữa, phân tích rủi ro có thể bao gồm việc sử dụng trường hợp đảm bảo.

8 Xác định mức toàn vẹn hệ thống hay sản phẩm

8.1 Giới thiệu

Việc xác định mức toàn vẹn hệ thống hay sản phẩm bao gồm các hoạt động sau:

a) Một phép đo tiêu chí rủi ro được định nghĩa, quy định cụ thể một phép đo hay tỉ lệ được sử dụng.

CHÚ THÍCH 1 "Tiêu chí rủi ro" được định nghĩa trong ISO/IEC 16085:2006 *Systems and software engineering - Life cycle process - Risk management* là: "thuật ngữ tham chiếu bởi ý nghĩa của rủi ro được đánh giá" và bao gồm chú thích sau: "Tiêu chí rủi ro có thể bao gồm chi phí và các lợi ích liên quan, các yêu cầu hợp pháp và theo luật định, các khía cạnh kinh tế-xã hội và môi trường, quan hệ giữa các bên liên quan, mức ưu tiên và đầu vào khác cho việc đánh giá."

CHÚ THÍCH 2 Một tính toán tiêu chí rủi ro có thể được chỉ ra theo các thuật ngữ của hệ quả tiêu cực nhiều lần theo khả năng phát sinh hay trong các thuật ngữ khác (ví dụ: tổn thất tối đa) và có thể là một kết hợp của các tính toán thành phần.

b) Các hạn chế cần thiết theo các giá trị tiêu chí rủi ro cho phép được xây dựng. Các hạn chế được yêu cầu thu được như một kết quả của việc phân tích và đánh giá rủi ro.

c) (Các) phép gán mức toàn vẹn cho sản phẩm hay hệ thống xuất phát từ các giới hạn này và việc đáp ứng chúng ám chỉ việc đáp ứng các giới hạn này về sự xuất hiện và định thời theo các hạn chế về độ không xác định. Do đó, mức toàn vẹn hệ thống hay sản phẩm tương ứng với các giá trị tiêu chí rủi ro cho phép.

CHÚ THÍCH 3 Trong cộng đồng an toàn, mức toàn vẹn có thể chỉ ra như "Yêu cầu Toàn vẹn nhấn mạnh việc sử dụng một tính toán tiêu chí rủi ro được ánh xạ cho các mức toàn vẹn (mà thường là một lượng rất nhỏ của tính toán tiêu chí rủi ro). Giới hạn tiêu chí rủi ro cho các ánh xạ hệ thống hay sản phẩm cho một mức toàn vẹn cụ thể cho hệ thống hay sản phẩm. (Do vậy, lần lượt tương ứng với các yêu cầu mức toàn vẹn - hoặc nghĩa vụ)"

8.2 Rủi ro

8.2.1 Giới thiệu

Đối với công năng của một phân tích rủi ro, thông tin cần thiết về hệ thống hay sản phẩm, môi trường, các yêu cầu bên liên quan, chiều rủi ro và các đặc tính tương ứng liên quan tới hệ thống hay sản phẩm. Ví dụ của các đặc tính liên quan bao gồm tính toàn vẹn, tính sẵn có, độ tin cậy và tính bảo mật cũng như các đặc tính liên quan tới việc sử dụng an toàn và kinh tế. Bất kỳ rủi ro nào được xác định bởi việc phân tích rủi ro và được phân tích theo hệ thống hay các giao diện sản phẩm; một mức toàn vẹn được gán cho hệ thống hay sản phẩm và giao diện của nó. Các mức toàn vẹn sản phẩm hay hệ thống này phản ánh các giá trị cần thiết của tiêu chí rủi ro tương ứng.

CHÚ THÍCH Mục tiêu vận hành tối thượng của việc tiếp cận các rủi ro và độ không xác định trong bộ tiêu chuẩn này là sự hiệu quả (hay ít nhất là sự bảo vệ) của các bên liên quan và tăng cường việc đưa ra quyết định của họ. Việc đạt được độ không xác định thấp hơn trong các thuật ngữ kỹ thuật đưa ra các nền tảng tốt hơn cho sự tin tưởng và các cơ sở cho việc đưa ra quyết định. Nói chung, khi độ không xác định liên quan tới kỹ thuật, sự tin tưởng bên liên quan là một trạng thái chủ quan có thể mang tính riêng biệt hay thậm chí phi lý. Do đó, nhằm đảm bảo việc sử dụng phù hợp các kết quả kỹ thuật, độ không xác định được đề cập tới trong tiêu chuẩn này thường có nhiều giá trị mục tiêu hơn mức tin tưởng bên liên quan chủ quan mà xuất phát từ việc sử dụng mức toàn vẹn.

8.2.2 Tiêu chí rủi ro

8.2.2.1 Đặc tả của tiêu chí rủi ro

Một tiêu chí rủi ro quy định ý nghĩa hay phương pháp đo lường rủi ro liên quan tới hệ thống hay sản phẩm và được sử dụng nhằm quy định các giới hạn rủi ro. Tiêu chí rủi ro này phải:

a) Được thực hiện theo tỷ lệ đo lường liên quan tới rủi ro.

b) Có các giới hạn được yêu cầu theo các giá trị được quy định cụ thể của nó.

c) Phù hợp với các yêu cầu quản lý, ví dụ: các yêu cầu hợp pháp, theo luật định hay hợp đồng bao gồm các giới hạn được xác định trong phần b).

Các đặc tả tiêu chí rủi ro này và bất kỳ các biện minh liên quan nào được đồng ý và xác nhận dựa trên Điều 11.

8.2.2.2 Phương pháp tính toán tiêu chí rủi ro

Các phương pháp được sử dụng cho việc tính toán tiêu chí rủi ro đưa ra các kết quả mà có thể được so sánh ngược lại với các đặc tả tiêu chí rủi ro. Càng đòi hỏi nhiều tình huống thì càng đáng tin, mạnh mẽ và phù hợp với tình huống mà các phương pháp được sử dụng cho việc tính toán tiêu chí rủi ro có thể. Khi đánh giá các phương pháp tính toán, các điều sau phải được văn bản hóa:

a) Các phương pháp và công cụ được sử dụng cho các tính toán tiêu chí rủi ro.
b) Các cách tiếp cận được sử dụng và kết quả của phương pháp và đánh giá công cụ.

Nhiều phương pháp tính toán tiêu chí rủi ro có thể được quy định cụ thể cho các trường hợp khác nhau. Các phương pháp bổ sung được chọn cần có các kết quả phù hợp hoặc kém hơn các phương pháp khác.

CHÚ THÍCH Các phương pháp được sử dụng cho việc tính toán tiêu chí rủi ro cần có một biện minh logic phản ánh việc mục đích sử dụng chúng. Biện minh này bao gồm sự tương hợp của độ tin cậy và sự vững chắc với các hệ quả liên quan, độ mới lạ, tính chặt chẽ của các đòi hỏi và các giới hạn về độ không xác định và trạng thái nghệ thuật liên quan.

8.2.3 Phân tích rủi ro

8.2.3.1 Tổng quan

Về cơ bản, việc phân tích rủi ro được thực hiện nhằm trả lời ba câu hỏi: điều gì có thể sai, khi nào và với hệ quả nào. Sự quan tâm cuối cùng là hệ quả tiêu cực. Phân tích rủi ro có thể bao trùm nhiều chiều rủi ro, ví dụ: an toàn, kinh tế và an ninh. Phạm vi được xác định theo Điều 7.3.1 có thể thực hiện các chiều được bao trùm. Các khía cạnh liên quan bao gồm khả năng của hệ thống hay sản phẩm, quan hệ của hệ thống hay sản phẩm với môi trường của nó và khả năng phân tích của hệ thống hay sản phẩm.

Mức toàn vẹn sản phẩm hay hệ thống tương ứng với các giá trị tiêu chí rủi ro cho phép. Sự xuất hiện và định thời của các điều kiện hay các hành vi (bao gồm lỗi) có thể ảnh hưởng tới giá trị đó trực tiếp hay gián tiếp hoặc bởi chức năng của nó bao gồm việc giảm nhẹ các hệ quả của sự kiện bắt đầu trong

các môi trường và điều kiện nguy hiểm. Điều kiện nguy hiểm là các điều kiện liên quan tới hệ thống hay sản phẩm, có thể dẫn đến các hệ quả tiêu cực.

CHÚ THÍCH 1 Kết quả phân tích và đánh giá rủi ro (xem Điều 8.2.4) có thể dẫn tới các thay đổi hệ thống hay thiết kế sản phẩm nhằm loại bỏ hay giảm thiểu rủi ro. Các thay đổi này có thể yêu cầu các hoạt động phân tích và/hoặc đánh giá rủi ro được lặp lại.

CHÚ THÍCH 2 Các phân tích và đánh giá rủi ro cần bao gồm lịch sử các tình huống giống hệt hay tương tự nhau, bao gồm các động cơ thúc đẩy đánh giá mức độ hoàn thiện của các kết quả. Theo thời gian, các động cơ thúc đẩy này phải được xây dựng một hiểu biết và trình diễn tăng cường theo tình huống. Các biên bản phải được lưu giữ thậm chí nếu chúng không thực nhu cầu.

8.2.3.2 Sự xuất hiện của phân tích rủi ro được yêu cầu

Phân tích và/hoặc đánh giá rủi ro phải được thực hiện:

a) Trước tiên, trước khi việc gán lần đầu tiên của một mức toàn vẹn hệ thống hay sản phẩm được đồng ý hay thừa nhận.

b) Bất kỳ khi nào các tình huống ảnh hưởng tới rủi ro được xác định có khả năng làm xấu đi hoặc không được xác định hay phân tích trước đó, được liệt kê trong Điều 6.7, ngoài ra việc phân tích tác động thể hiện việc phân tích rủi ro là không cần thiết.

c) Bất kỳ khi nào một giao diện hệ thống hay phần mềm phụ thuộc vào các thay đổi môi trường, ngoài ra việc biện minh văn bản hóa được nêu ra cho việc làm điều gì đó khác.

Sau khi triển khai hệ thống hay thiết kế phần mềm, việc xác nhận phải thu được rằng các mức toàn vẹn được gán cho hệ thống hay các giao diện sản phẩm phản ánh các giá trị tiêu chí rủi ro được yêu cầu.

8.2.3.3 Xác định hệ quả tiêu cực có thể

Các hệ quả tiêu cực liên quan tới hệ thống phải được xác định và đánh giá.

CHÚ THÍCH Nhằm bổ sung cho các hệ quả tiêu cực bên ngoài, các phần tử hệ thống có thể dẫn tới các hệ quả tiêu cực “bên trong” (ví dụ: việc ngắt quãng thông tin)

8.2.3.4 Xác định điều kiện nguy hiểm

Các điều sau phải được đồng ý và thừa nhận dựa trên Điều 11:

a) Các điều kiện, hành vi và sự kiện liên quan và quan hệ giữa chúng.
b) Biện minh cho việc xác định là liên quan (hoặc trong một vài trường hợp không liên quan).

Các điều kiện tương ứng với hệ thống hay sản phẩm có thể dẫn tới các hệ quả tiêu cực (các điều kiện nguy hiểm) cần được xác định cùng với các sự kiện bắt đầu của chúng.

CHÚ THÍCH 1 Một điều kiện được xác định có thể được phép, tạo cơ hội, gây ra, ngăn chặn sự chống hay giảm thiểu, thay đổi hay góp phần vào các hệ quả tiêu cực hoặc chuyển đổi từ một (nhiều) điều kiện nguy hiểm khác.

CHÚ THÍCH 2 Một sự kiện, điều kiện nguy hiểm không được mong muốn hay việc chuyển đổi giữa các điều kiện có thể có một độ không xác định phát sinh tương ứng. Chuỗi điều kiện và/hoặc sự kiện có thể dẫn tới một điều kiện tiên quyết trung gian cho một hệ quả tiêu cực tuân theo một hệ quả tiêu cực thực tế. Điều kiện tiên quyết cho một hệ quả tiêu cực có thể là sự kết hợp của "điều kiện" được xác định trong các phân tích có thể cần thiết nhằm phát sinh đồng thời hoặc định thời hiện tại.

Trong ngữ cảnh này, các điều kiện nguy hiểm tương ứng với một hệ thống hay sản phẩm nếu:

a) Lỗi phần mềm hay hệ thống có thể dẫn tới điều kiện nguy hiểm.
b) Việc vận hành hệ thống hay sản phẩm trong phạm vi áp dụng đòi hỏi mức toàn vẹn hoặc sự tham gia trong các quy trình vòng đời khác có thể dẫn tới một điều kiện nguy hiểm.
c) Hệ thống hay sản phẩm thực hiện một giảm thiểu chức năng cho một sự kiện bắt đầu trong môi trường có thể dẫn tới điều kiện nguy hiểm.
d) Việc hành xử hay vận hành như đã quy định dẫn tới điều kiện nguy hiểm, nhưng kết quả của các quyết định cố ý được tạo ra với cảnh báo rằng điều này có thể xảy ra.

CHÚ THÍCH 3 Các lỗi có thể thay đổi theo các hệ quả tiêu cực tiềm ẩn; một vài lỗi có thể không đáng kể. Tuy nhiên, trong việc xác định các thay đổi đó, tất cả lỗi cần được xem xét cũng như dải sự kiện và điều kiện có thể xảy ra. Các điều kiện và sự kiện trong môi trường bị ảnh hưởng bởi một hệ thống hay sản phẩm có thể thay đổi tác động của nó trong tình huống dự kiến.

Các điều kiện nguy hiểm bất ngờ có thể xảy ra và các sự kiện bắt đầu có thể không rõ ràng. Các điều kiện nguy hiểm phải được xem xét bất kể cách thức các điều kiện nguy hiểm đó phát sinh.

8.2.3.5 Xem xét kiến trúc hệ thống hay sản phẩm

Kiến trúc hệ thống hay sản phẩm (khi sẵn có) phải phân chia theo điều kiện nguy hiểm và việc xác định sự kiện nhằm đảm bảo rằng các chế độ lỗi, hành vi, điều kiện, thuộc tính đặc trưng với công nghệ sử dụng và các tương tác với môi trường được xem xét.

CHÚ THÍCH 1 Đây là công nghệ điều tra không xung đột với các yêu cầu trong Điều 8.4 mà mức toàn vẹn hệ thống hay sản phẩm không phụ thuộc vào kiến trúc bên trong của nó.

CHÚ THÍCH 2 Như thành phần, các nhà phân tích và thiết kế thường giải quyết các kết quả phân tích rủi ro, hệ quả tiêu cực tiềm ẩn và các điều kiện nguy hiểm được xác định trong khi tạo ra hoặc thay đổi một thiết kế hệ thống sau này hoặc các thủ tục vận hành hay duy trì của nó.

8.2.3.6 Phân tích hệ quả

Phân tích hệ quả được sử dụng nhằm đánh giá độ nghiệm trọng của một điều kiện nguy hiểm liên quan tới việc xuất hiện các hệ quả tiêu cực. Các đo lường có thể giảm thiểu hệ quả tiêu cực của (các) sự kiện bắt đầu hay các điều kiện nguy hiểm phải được xác định. Thảo luận liên quan xem Điều 7.3.4.

8.2.3.7 Phân tích định thời và sự xuất hiện

Phân tích độ không xác định, định thời và sự xuất hiện được sử dụng nhằm đánh giá khả năng của mỗi hệ quả, điều kiện nguy hiểm hay sự kiện bắt đầu.

Việc định thời cho các điều kiện (ví dụ: sự xuất hiện và thời hạn) hoặc sự xuất hiện sự kiện (ví dụ: tần suất) phải được đánh giá nhằm đáp ứng bất kỳ yêu cầu nào về độ không xác định của kết quả. Đánh

giá này cần sử dụng nhiều nguồn, bao gồm dữ liệu lịch sử, các kết quả đồng bộ theo các công nghệ kỹ thuật hay phân tích (xem TCVN 10607-1 với các tham chiếu liên quan) và các đánh giá liên quan được bắt nguồn từ theo việc biện minh của chuyên gia.

CHÚ THÍCH Kết quả phân tích có thể được nhấn mạnh trong các thuật ngữ định lượng và chất lượng như các thuật ngữ cho các dải tần số (ví dụ: Tần số, Có thể xảy ra, Thường xuyên, Từ xa, Không thể xảy ra hoặc Không thể tưởng tượng) như các yêu cầu cho việc so sánh với tiêu chí rủi ro được đáp ứng.

8.2.3.8 Sử dụng trường hợp đảm bảo xác định mức toàn vẹn hệ thống hay sản phẩm

Khi một hay một phần hoàn thiện của trường hợp đảm bảo là sẵn có trong quá trình phân tích rủi ro, việc sử dụng có thể hữu ích cho việc xác lập các giới hạn tương ứng với hệ thống hay sản phẩm trong quá trình phân tích rủi ro và cho việc xác thực của việc xác định các đặc tính theo đòi hỏi mức toàn vẹn.

CHÚ THÍCH Trong các trường hợp đảm bảo và mức toàn vẹn tưởng ứng, các đòi hỏi liên quan có thể được ánh xạ đối với mỗi đòi hỏi khác.

8.2.4 Đánh giá rủi ro

Kết quả của việc phân tích và đánh giá rủi ro bao gồm các giới hạn được yêu cầu theo sự xuất hiện, định thời và các giá trị hệ quả, điều kiện và độ không xác định tương ứng theo các yêu cầu hệ thống hay sản phẩm mà phát sinh.

Các điều sau phải được thực hiện:

a) Triển khai các giới hạn được yêu cầu theo sự xuất hiện và định thời của các hành vi và/hoặc điều kiện hệ thống hay sản phẩm và độ không xác định cho phép tương ứng theo sự phù hợp các giới hạn này.

b) Xem xét khả năng của các hành vi hay điều kiện tương ứng với hệ thống hay sản phẩm, hơn là hệ thống hay sản phẩm hay các phần tử của nó không đáp ứng được các đặc tả, dẫn đến tiêu chí rủi ro không đáp ứng được.

Đánh giá rủi ro và kết quả của nó được đồng ý và thừa nhận dựa trên Điều 11.

CHÚ THÍCH Không điều gì trong tiêu chuẩn này được biên dịch như việc yêu cầu hay cho phép gán các mức toàn vẹn mà tiêu chí rủi ro tương ứng với hệ thống hay sản phẩm không đáp ứng được.

8.3 Gán mức toàn vẹn hệ thống hay sản phẩm

Các giới hạn được yêu cầu theo sự xuất hiện, định thời và giá trị của các hệ quả, điều kiện và độ không xác định tương ứng theo phân tích và đánh giá rủi ro cần được sử dụng nhằm xác lập các giới hạn được yêu cầu theo sự xuất hiện và định thời của các hành vi hệ thống hay sản phẩm. Một mức toàn vẹn có thể được gán cho toàn bộ hệ thống hay sản phẩm, do đó tất cả các giao diện hay một mức toàn vẹn khác biệt liên quan có thể được gán cho mỗi giao diện. Trong trường hợp sau, mức toàn vẹn cũng áp dụng cho hệ thống hay phần tử sản phẩm cài đặt giao diện đó.

Một hay nhiều mức toàn vẹn được gán phải có các đòi hỏi mức toàn vẹn nhằm đáp ứng các giới hạn bắt nguồn từ các hành vi hệ thống hay sản phẩm. Nhằm đạt được điều này, ít nhất một trong các điều sau là cần thiết:

a) Đáp ứng hệ thống hay sản phẩm được gán mức toàn vẹn nhằm chỉ ra việc đáp ứng các giới hạn được yêu cầu theo các hành vi hệ thống hay sản phẩm.

b) Mức toàn vẹn hệ thống hay sản phẩm phù hợp với sự đáp ứng các giới hạn được yêu cầu theo các hành vi hệ thống hay sản phẩm mà không ám chỉ chúng. Các phương pháp khác được sử dụng sau đó nhằm cung cấp thông tin cần thiết nhằm thể hiện các hành vi thực tế của hệ thống hay sản phẩm đáp ứng các giới hạn được yêu cầu theo các hành vi theo các giới hạn được yêu cầu về độ không xác định. Các phương pháp khác, kết quả và tài liệu của chúng được đồng ý và thừa nhận dựa trên Điều 11.

CHÚ THÍCH Một vài hệ thống, sản phẩm hay các giao diện phần tử có thể không có sự phụ thuộc hay liên hệ liên quan tới mức toàn vẹn giữa chúng bởi các thực thể bên ngoài. Trong khi các giao diện này không cần gán một mức toàn vẹn, các giao diện này ít nhất phải được gán cho mức toàn vẹn thấp nhất.

8.4 Sự độc lập của kiến trúc nội bộ

Mức toàn vẹn hệ thống hay sản phẩm hoặc sự độc lập được yêu cầu tại giao diện bên ngoài không phải phụ thuộc vào kiến trúc nội bộ hệ thống hay sản phẩm. Theo mục đích này, hệ thống và sản phẩm phải được coi như một hộp đen.

8.5 Duy trì mức toàn vẹn hệ thống hay sản phẩm

8.5.1 Giới thiệu

Lí do cho việc tái thiết lập mức toàn vẹn được phân thành ba mục: (1) Thay đổi hệ thống (2) Một rủi ro chưa xác định được biết đến và (3) Yêu cầu người dùng thay đổi.

8.5.2 Thay đổi hệ thống

Nhu cầu cho việc tái thiết mức toàn vẹn hệ thống hay sản phẩm phải được đánh giá và nếu cần thiết, việc tái thiết dựa trên tiêu chuẩn này bất kỳ khi nào một thay đổi hệ thống hay sản phẩm được đề xuất hay triển khai.

8.5.3 Rủi ro đã biết

Nhu cầu nhằm tái thiết mức toàn vẹn hệ thống hay sản phẩm phải được đánh giá và nếu cần thiết, việc tái thiết dựa trên tiêu chuẩn này bất kỳ khi nào mà:

a) Một phân tích hay đánh giá rủi ro tồn tại mà không được phản ánh trong quyết định cuối cùng: gán mức toàn vẹn hệ thống hay sản phẩm.
b) Một quyết định được tạo ra giữa các thiết kế thay thế và các giá trị tiêu chí rủi ro cần thiết khác nhau.
c) Hệ thống hay sản phẩm được khám phá mới hoặc các cơ hội bị nghi ngờ cho các điều kiện nguy hiểm, sự vi phạm các đòi hỏi liên quan hoặc việc làm xấu đi hệ quả tiêu cực tương ứng.
d) Các lỗi phát sinh mà không kịp thời điều chỉnh.

e) Các nguy hiểm hay lỗi mới được khám phá hay bị nghi ngờ tồn tại hoặc được chỉ ra bởi dữ liệu vận hành.
f) Thiết kế hệ thống hay sản phẩm, hoặc các thay đổi chức năng bao gồm việc giảm thiểu (ví dụ: loại bỏ, phòng ngừa hay tránh, hạn chế, giảm thiểu hoặc quản lý) các hệ quả.
g) Thiết kế hệ thống hay sản phẩm không dẫn tới việc đáp ứng tiêu chí rủi ro.

8.5.4 Thay đổi yêu cầu

Sự cần thiết nhằm tái thiết mức toàn vẹn hệ thống hay sản phẩm phải được đánh giá và nếu cần thiết, việc tái thiết dựa trên tiêu chuẩn này bất kỳ khi nào các yêu cầu người dùng hệ thống thay đổi.

8.6 Khả năng truy xuất của việc gán mức toàn vẹn hệ thống hay sản phẩm

Việc gán các mức toàn vẹn giao diện sản phẩm hay hệ thống phải được truy xuất theo các giới hạn từ việc đánh giá rủi ro, phương pháp sử dụng và công năng thực tế của việc xác định chúng.

9 Gán mức toàn vẹn phần tử hệ thống

9.1 Giới thiệu

Một sản phẩm hay hệ thống bao gồm một hay nhiều phần tử. Một phần tử có thể chỉ là phần mềm, chỉ là phần cứng, bao gồm các thực thể khác, hoặc kết hợp giữa chúng. Các phần tử có thể bị phụ thuộc (được sử dụng) bởi nhiều phần tử và có thể phụ thuộc (sử dụng) nhiều phần tử.

Hành vi giao diện liên quan tới việc đạt được mức toàn vẹn phụ thuộc trực tiếp hay gián tiếp vào các phần tử sản phẩm hay hệ thống cài đặt giao diện đó. Một khi các mức toàn vẹn được thiết lập cho giao diện - theo cả hình thức cho hệ thống hay sản phẩm hoặc riêng lẻ - các mức toàn vẹn cần được thiết lập cho các phần tử đó. Các phép gán liên quan tới phần tử này có thể phức tạp bởi không có khả năng gán các mức toàn vẹn mới cho các phần tử hiện có. Hơn nữa, khả năng tồn tại cho các phần tử dẫn tới các hệ quả tiêu cực “nội bộ” (ví dụ: sự phá hủy vật lý cho một hệ thống) ảnh hưởng tới các phép gán mức toàn vẹn.

Gán các mức toàn vẹn cho các phần tử hệ thống hay sản phẩm dựa trên việc thiết kế hệ thống hay sản phẩm và các phần tử của nó. Đặc tính trong một đòi hỏi mức toàn vẹn của một phần tử hệ thống thường tương tự như của các phần tử phụ thuộc vào nó. Tuy nhiên, mối quan hệ này có thể bị ảnh hưởng bởi (các) vai trò của phần tử trong thiết kế.

9.2 Kiến trúc và thiết kế

9.2.1 Tổng quan

Kiến trúc và thiết kế của hệ thống, sản phẩm hay phần tử phụ thuộc vào phần tử hệ thống được gán một mức toàn vẹn, phải:

a) Được định nghĩa chi tiết đầy đủ trước khi gán các mức toàn vẹn nhằm cho phép việc định danh vai trò của phần tử và giao diện của chúng và tạo ra cơ sở cần thiết cho việc định danh các phụ thuộc liên quan.

b) Cho phép xác minh các phụ thuộc đó.

Đối với cách tiếp cận các mức toàn vẹn thể hiện ở đây là hiệu quả nhất, khả năng phân tích hệ thống hay sản phẩm và các phần tử của nó liên quan tới một hay nhiều đặc tính tương ứng cần được đảm bảo hoặc xác nhận.

CHÚ THÍCH Xem xét phải được đưa ra cho khả năng thiết kế nhằm thực hiện các phép gán mức toàn vẹn được đưa ra.

9.2.2 Cơ chế xử lý lỗi

Cơ chế xử lý lỗi bao gồm một hay nhiều phần tử hệ thống có thể được sử dụng nhằm dò tìm các lỗi của phần tử sản phẩm hay hệ thống, đưa ra hành động nhằm ngăn chặn các hệ quả không được phép. Trong thường hợp này, lỗi phần tử sản phẩm hay hệ thống vẫn đáng quan tâm nếu lỗi xảy ra và cơ chế xử lý lỗi không hiệu quả. Ví dụ của cơ chế xử lý lỗi bao gồm các kiểm tra tính toàn vẹn dữ liệu (phần mềm), bộ định thời phần cứng (phần cứng) và việc phục hồi thủ công (con người). Các đặc trưng thiết kế như: sự dư thừa, đa dạng và phân định (ví dụ: sự phân định theo thời gian và không gian, phân vùng, kiểm soát tương tác, sự tách rời, các rào cản, không can thiệp, bảo vệ hoặc cô lập) có thể ảnh hưởng tới mức toàn vẹn cần thiết của các phần tử hệ thống.

CHÚ THÍCH 1 Tính dư thừa có thể được sử dụng nhằm ngăn chặn các lỗi từ việc dẫn tới các điều kiện nguy hiểm, miễn là các lỗi chế độ phổ biến giữa các phần tử dư thừa được ngăn ngừa (ví dụ: bởi sự đa dạng thích hợp giữa chúng)

CHÚ THÍCH 2 Xem xét thiết kế phải được đưa ra cho các khả năng cho độ tin cậy và khả năng đáp ứng, sự phát hiện và cảnh báo sớm, sự hạn chế, phá hủy, chuẩn đoán và sửa chữa, cung cấp cảnh báo tình huống liên tục, tạo ra các quyết định nhanh chóng khi khẩn cấp và phục hồi nhanh chóng, kết hợp với môi trường, theo sự xuất hiện các điều kiện nguy hiểm và hệ quả tiêu cực. Xem Điều 9.5.2.

9.3 Gán

Mỗi phần tử hay giao diện phần tử hệ thống phụ thuộc vào các phần tử hệ thống cũng được gán các mức toàn vẹn hoặc tạo ra giao diện bên ngoài cho hệ thống và sản phẩm mà các thực thể phụ thuộc phải được gán một mức toàn vẹn, sử dụng một phương thức phù hợp với:

a) Các đặc tả mức toàn vẹn được sử dụng và việc biện minh cho các yêu cầu mức toàn vẹn.

b) Các phụ thuộc liên quan.

c) Các yêu cầu theo Điều 9.5.2 và 9.5.3.

d) Các mức toàn vẹn thấp hơn được phép chỉ bởi việc sử dụng các đặc trưng thiết kế mà đã được đồng ý và thừa nhận dựa theo Điều 11, chỉ trong các giới hạn được chấp nhận và thừa nhận. Ví dụ: việc xem xét mức độ lợi ích được tạo ra bởi một cơ chế xử lý lỗi và việc xác định điều tạo thành sự đa dạng tương ứng.

CHÚ THÍCH 1 Nói chung, việc kết hợp vai trò của mỗi phần tử và các mức toàn vẹn phần tử đó cần dẫn tới việc đạt được mức toàn vẹn được gán cho một phần tử (các giao diện của nó). Một phần tử với nhiều phụ thuộc của nó liên quan tới một tập mức toàn vẹn cần được gán mức toàn vẹn cao nhất giữa chúng, ngoại trừ được cung cấp bởi các xem xét đặc biệt và sự cho phép của tiêu chuẩn này.

CHÚ THÍCH 2 Các mục mà cần được đảm bảo theo thiết kế, triển khai, vận hành và bằng chứng liên quan và (1) việc đối mặt xảy ra với một hay nhiều thực thể thích hợp, (2) các thực thể này có các hành vi đối mặt thích hợp và (3) tính toàn vẹn

được duy trì giữa các kết nối. Các mục này thường bao gồm các mối quan tâm liên quan tới các thuộc tính và hành vi của một cơ chế thiết lập kết nối (ví dụ: hạ tầng kết nối). Các mục này đôi khi được gọi là “sự toàn vẹn giao diện”.

9.4 Phạm vi gán

Việc gán các mức toàn vẹn phải được thực hiện cho một phạm vi phù hợp với các yêu cầu mức toàn vẹn, liên quan tới tập các đặc tả mức toàn vẹn và biện minh của các yêu cầu mức toàn vẹn. Phạm vi này được đồng ý và thừa nhận dựa theo Điều 11.

9.5 Lưu ý đặc biệt

9.5.1 Vòng và đệ quy

Mạng được tạo thành bởi các quan hệ phụ thuộc có thể bao gồm các vòng. Nếu một vòng (hay đệ quy) tồn tại, thì:

a) Các phương pháp áp dụng phải bao trùm hoàn toàn số lượng các vòng hay mức đệ quy có thể.

b) Tài liệu phải được cung cấp cho các phương pháp này và có thể được cung cấp với việc định nghĩa mức toàn vẹn.

Đối với các vòng và đệ quy, các công cụ tự động cần được sử dụng nhằm thực hiện và/hoặc kiểm tra các phương pháp sử dụng.

9.5.2 Tình huống đặc biệt và yêu cầu liên quan tới mức toàn vẹn

Với các tình huống sau, các yêu cầu/hướng dẫn và khuyến nghị bổ sung được áp dụng:

a) Nếu bên đảm bảo tính toàn vẹn đánh giá các hệ quả tiềm ẩn là quan trọng hay nghiêm trọng, thì tính chính xác, sự hoàn thiện và chiều sâu của các phân tích và xác minh phải biện minh tương ứng với các hệ quả đó.

b) Nếu trạng thái hành vi (bao gồm lỗi) của bất kỳ phần tử nào, trong việc cô lập hay kết hợp trạng thái của các phần tử khác, dẫn tới tình trạng không gửi được của một chức năng giảm thiểu - cụ thể hơn, thường không được gọi khi cần thiết hoặc không sẵn có, thực hiện chính xác khi được gọi - các phân tích phải bao gồm các phát sinh nhu cầu cho chức năng giảm thiểu và các hệ quả của việc không gửi được của nó.

c) Nếu các mức toàn vẹn được gán bất kỳ đâu trong hệ thống hay sản phẩm, thì ít nhất các yêu cầu mức toàn vẹn tương ứng phải được bắt buộc trong việc tương tác giữa các phần tử bao gồm các phần tử đó mà không được gán các mức toàn vẹn.

d) Nơi mà không mức toàn vẹn nào được thể hiện cho các phần tử hệ thống hiện thời và bằng chứng được yêu cầu theo các yêu cầu mức toàn vẹn của mức toàn vẹn được gán hiện tại là không sẵn có, các thay đổi trong Điều 10.2 được áp dụng.

9.5.3 Các hành vi khác với lỗi

Một xem xét hệ thống hay sản phẩm phải đưa ra khả năng mà các hành vi không được phân loại như các lỗi trong đặc tả được văn bản hóa cho một phần tử có thể tuy nhiên gây ra cho hệ thống hay sản phẩm hay bất kỳ phần tử nào không đáp ứng được mức toàn vẹn được gán hay kết quả của các điều

kiện nguy hiểm hay hệ quả tiêu cực của nó. Nói cách khác, các điều kiện mà không phải là sai sót cũng có thể làm như vậy.

9.6 Duy trì việc gán mức toàn vẹn

9.6.1 Tổng quan

Việc gán các mức toàn vẹn phải được duy trì. Nếu một hệ thống, sản phẩm hay thiết kế phần tử được điều chỉnh, thay đổi xuất hiện trong hệ thống hay môi trường sản phẩm, hoặc các phân tích hay đánh giá rủi ro mới hay được điều chỉnh được thực hiện, các mức toàn vẹn có thể cần tái gán. Việc tái gán có thể bao gồm việc gán mới, các mức toàn vẹn cao hơn bất kỳ khi nào được yêu cầu.

9.6.2 Thay đổi gán mức toàn vẹn

Cụ thể hơn, nhu cầu cho một gia tăng mức toàn vẹn được gán cho một hệ thống, sản phẩm hay phần tử phải được đánh giá và mức toàn vẹn được gán lại nếu bất kỳ lúc nào cần thiết:

a) Phân tích hay đánh giá rủi ro chỉ ra một gia tăng rủi ro của các hệ quả tiêu cực, điều kiện nguy hiểm hoặc số lượng các phát sinh hay đưa ra bất kỳ chỉ báo nào khác về mức toàn vẹn của một phần tử hệ thống có thể yêu cầu một gia tăng.

b) Một điều chỉnh thiết kế cho một phần tử hệ thống có thể yêu cầu một gia tăng theo mức toàn vẹn được gán cho phần tử đó, ví dụ: việc gỡ bỏ dư thừa hay lưu trữ dự phòng.

c) Các gia tăng giá trị tiêu chí rủi ro khả dụng của một hệ thống hay sản phẩm được xác định.

d) Thiết kế sản phẩm hay hệ thống không dẫn tới việc đáp ứng tiêu chí rủi ro.

e) Thiết kế của một phần tử hệ thống không dẫn tới việc đáp ứng mức toàn vẹn cần thiết của nó.

f) Mức chống chịu cho các suy giảm giá trị tiêu chí rủi ro liên quan hoặc giới hạn về các giá trị tiêu chí rủi ro cần thiết thay đổi theo cách thức mà không làm suy yếu nó.

Việc thay đổi các phân định mức toàn vẹn, đặc biệt cho một mức toàn vẹn cao hơn có thể yêu cầu các hoạt động bổ sung, bao gồm các phân tích có thể được điều khiển cho mức toàn vẹn thấp hơn.

10 Đáp ứng yêu cầu mức toàn vẹn

10.1 Yêu cầu liên quan tới bằng chứng

10.1.1 Thông tin liên quan

Bằng chứng phải bao gồm hoặc được đi kèm bởi việc bao trùm thông tin của:

a) Định nghĩa.

b) Tính toàn vẹn, hiệu lực, chính xác và việc đạt được các giới hạn về độ không xác định cần thiết.

c) Việc xác định các yêu cầu mức toàn vẹn mà bằng chứng góp phần nhằm đáp ứng sự quan trọng và ý nghĩa của bằng chứng trong ngữ cảnh đó.

d) Sự liên quan của ngữ cảnh theo bằng chứng được thu thập hay tạo ra.

e) Một hay nhiều phiên bản hoặc các trường hợp của hệ thống, sản phẩm hay phần tử liên quan tới nó.

f) Con người và các công cụ tạo ra bằng chứng.

g) Các giả định liên quan.

h) Sự phù hợp với các tiêu chuẩn liên quan, ngoại trừ khi việc biện minh được văn bản hóa được tạo ra để làm điều gì khác.

i) Nguồn hay phương thức truy nguyên.

j) Việc cho phép truy cập bằng chứng và thông tin đi kèm.

k) Lịch sử của bằng chứng.

CHÚ THÍCH 1 Bằng chứng liên quan có thể bao gồm bằng chứng về cách thức một yêu cầu mức toàn vẹn được đáp ứng và bằng chứng hỗ trợ thông tin được liệt kê bên trên.

CHÚ THÍCH 2 Ví dụ của bằng chứng bao gồm một biên bản của các việc đạt được trong quá khứ của các hệ thống liên quan, một kết quả của việc xác minh quy trình và một báo cáo của việc đánh giá hoàn toàn tổ chức của người vận hành hay người bảo dưỡng.

10.1.2 Tổ chức bằng chứng

Tập bằng chứng, các mục nó bao gồm và thông tin đi kèm phải được tổ chức, định vị và được trình bày để có thể hiểu được và thỏa mãn mục đích của cá nhân đánh giá, thừa nhận và sử dụng chúng.

10.1.3 Biên dịch bằng chứng

Bất kỳ khi nào các biên dịch hợp pháp tồn tại của bằng chứng liên quan nhằm đáp ứng các yêu cầu mức toàn vẹn, một biên dịch xem xét thận trọng việc đạt được này phải được sử dụng. Việc biên dịch yếm thế phải được xem xét.

10.2 Thay thế

Đối với tất cả mức toàn vẹn được gán cho một hệ thống, sản phẩm hay phần tử, các yêu cầu mức toàn vẹn tương ứng phải được đáp ứng nếu có thể thực hành. Nếu toàn bộ bằng chứng được yêu cầu bởi các yêu cầu mức toàn vẹn không thể thay thế không được phép thay đổi; thì:

a) Hệ thống, sản phẩm hay phần tử phải được thể hiện nhằm đáp ứng mức toàn vẹn được gán theo các giới hạn được yêu cầu về độ không xác định bởi việc sử dụng bằng chứng và phân tích liên quan.

b) Bất kỳ các cách thức thay đổi nào (một trường hợp đảm bảo có thể coi như một vai trò) phải được văn bản hóa, có biện minh được văn bản hóa, bao gồm một phân tích rủi ro của việc sử dụng, được đồng ý và thừa nhận dựa trên Điều 11.

10.3 Đạt được đòi hỏi mức toàn vẹn

Một đòi hỏi mức toàn vẹn phải được xác định không đạt được nếu bằng chứng thu được liên quan tới các yêu cầu mức toàn vẹn:

a) Thể hiện một yêu cầu mức toàn vẹn không được đáp ứng.

b) Không hoàn thiện và bất kỳ thay đổi nào là không thành công. Xem Điều 10.2.

c) Không kết thúc hoặc thất bại nhằm đáp ứng các giới hạn được yêu cầu về độ không xác định.

Cho tất cả mức toàn vẹn được gán, việc đáp ứng toàn bộ tập yêu cầu mức toàn vẹn và thu thập bằng chứng (bao gồm các thay đổi được thừa nhận theo Điều 10.2) phải được:

d) Bao gồm rõ ràng theo các kế hoạch, bao gồm các tài nguyên và thời gian cần thiết.

e) Nhất quán với tất cả kế hoạch.

10.4 Hành động hiệu chỉnh

Các vấn đề iiên quan tới mức toàn vẹn được báo cáo phải:

a) Được ghi lại và các hành động liên quan được theo dõi.

b) Có các hành động hiệu chỉnh cần thiết diễn ra theo thời gian tương ứng với mức độ nghiêm trọng và tác động vào các giá trị tiêu chí rủi ro.

c) Không có các hành động hiệu chỉnh dẫn tới sự vi phạm các giới hạn liên quan tới mức toàn vẹn hay các yêu cầu bao gồm các điều đó trong tiêu chuẩn này, ngoại trừ tạm thời trong quá trình các điều kiện khẩn cấp được biện minh theo một lý do được văn bản hóa (ví dụ: việc phân tích và đánh giá rủi ro) và được đồng ý và thừa nhận dựa trên Điều 11.

11 Thỏa thuận và phê duyệt

11.1 Thẩm quyền

Các vai trò sau phải được xác định và kết nối với các bên liên quan:

a) Các bên phê duyệt được yêu cầu cho một sử dụng cụ thể tiêu chuẩn này:

   1) Bên phê duyệt cho việc định nghĩa các mức toàn vẹn (yêu cầu cho việc định nghĩa mức toàn vẹn)
   2) Bên phê duyệt cho việc sử dụng các mức toàn vẹn (yêu cầu cho việc sử dụng mức toàn vẹn)

CHÚ THÍCH 1 Được định nghĩa trong TCVN 10607-1, bên phê duyệt là một (hay nhiều) cá nhân và/hoặc một (hay nhiều) tổ chức) chịu trách nhiệm phê duyệt các hoạt động, tạo tác và các khía cạnh khác được bao trùm bởi các nội dung liên quan của tiêu chuẩn này.

b) Bên đảm bảo tính toàn vẹn (cho việc sử dụng mức toàn vẹn)

CHÚ THÍCH 2 Được định nghĩa trong TCVN 10607-1, bên đảm bảo tính toàn vẹn là cá nhân hay tổ chức chịu trách nhiệm cho việc chứng nhận sự tuân thủ các yêu cầu mức toàn vẹn. Bên đảm bảo mức toàn vẹn có thể giống với bên phê duyệt nếu các yêu cầu liên quan tới nó được đáp ứng, ví dụ: sự phụ thuộc (xem Điều 11.4)

c) Bên thiết kế (yêu cầu cho việc sử dụng mức toàn vẹn)

CHÚ THÍCH 3 Được định nghĩa trong TCVN 10607-1, bên thiết kế là cá nhân hay tổ chức chịu trách nhiệm cho việc sản xuất thiết kế hệ thống.

CHÚ THÍCH 4 Các thẩm quyền được yêu cầu cho việc sản xuất và bảo trì, có thể được yêu cầu trong suốt vòng đời.

11.2 Thỏa thuận và phê duyệt cụ thể liên quan tới định nghĩa mức toàn vẹn

Bên phê duyệt đối với việc định nghĩa các mức toàn vẹn phải thừa nhận các kết quả định nghĩa hoạt động, bao gồm đòi hỏi, (các) yêu cầu mức toàn vẹn và việc biện minh liên quan với chúng, (các) tài liệu và văn bản cho mỗi mức toàn vẹn: việc nhóm các mức toàn vẹn thành các tập mức toàn vẹn, bao gồm trình tự của chúng; và tương xứng với tập các mức toàn vẹn của phạm vi áp dụng.

11.3 Thỏa thuận và phê duyệt cụ thể liên quan tới sử dụng mức toàn vẹn

Bên thiết kế và bên đảm bảo tính toàn vẹn phải tuân thủ các quyết định, khía cạnh và tạo tác sau:

a) Việc xác định các chiều rủi ro liên quan.

b) Các mức toàn vẹn đặc trưng được sử dụng.

c) Khả năng phù hợp của một mức toàn vẹn cho việc sử dụng trong việc hiện diện tiềm ẩn của các thất bại có hệ thống và bất kỳ biện minh nào của việc sử dụng mà không được yêu cầu.

d) Quy trình quyết định cho việc gán mức toàn vẹn.

e) Sự an toàn của bất kỳ lỗi, sai sót, hay phát sinh thất bại và cô lập nào.

f) Cả:

   1) Mức lợi ích được phép cho trường hợp sử dụng cụ thể hay trường hợp sử dụng kết hợp cụ thể thay thế của các đặc trưng thiết kế và kiến trúc.
   2) Phương pháp quyết định cho việc triển khai lợi ích của một đặc trưng thiết kế và kiến trúc hoặc các kết hợp của chúng.

g) Bất kỳ phân loại nào của các đặc trưng thiết kế hay kiến trúc.

h) Các phương pháp cho việc thể hiện sự đạt được đòi hỏi mức toàn vẹn được gán nếu toàn bộ bằng chứng cần thiết theo lĩnh vực cho mức toàn vẹn này không thể thu được và các phương pháp đó có thể được sử dụng.

i) Các quyết định phù hợp với các tiêu chuẩn khác sẽ dẫn tới việc đáp ứng một phần hay khía cạnh của tiêu chuẩn này.

Bên đảm bảo tính toàn vẹn phải thừa nhận các khía cạnh sau:

a) Tiêu chí rủi ro cà tất cả các thay đổi với nó.

b) Sự quan tâm được đưa ra cho khả năng của các hành vi hay điều kiện thay thế tương ứng với hệ thống hay sản phẩm hơn là thất bại phần tử hệ thống hay hệ thống hoặc thất bại sản phẩm dẫn tới hệ thống hay sản phẩm không đáp ứng được tiêu chí rủi ro, các kế hoạch và kết quả của sự quan tâm này.

c) Phạm vi hay các điều kiện theo tiêu chuẩn này áp dụng cho bất kỳ thay đổi phạm vi hay điều kiện nào theo mức toàn vẹn áp dụng. Nhà thiết kế phải được xem xét trong quy trình phê duyệt.

d) Các quyết định mà một rủi ro là không đáng kể hoặc không được phân tích hay đánh giá.

e) Các cách tiếp cận được chọn lựa cho việc trình bày mức toàn vẹn.

f) Mức toàn vẹn được gán cho hệ thống hay sản phẩm.

g) (Các) quyết định mà tiêu chí rủi ro được đáp ứng.

Bên đảm bảo tính toàn vẹn và nhà thiết kế phải cùng thừa nhận các khía cạnh sau:

a) Phạm vi của tập phần tử hệ thống được gán mức toàn vẹn.

b) Các phân định mức toàn vẹn cho các phần tử hệ thống.

c) Các kết quả phân tích và đánh giá rủi ro.

d) Bất kỳ mức toàn vẹn nào mà không bao trùm các thất bại và/hoặc sự nguy hại có hệ thống.

Tất cả thẩm quyền đưa ra việc chứng nhận hay phê duyệt việc sử dụng hệ thống hay sản phẩm cũng như người quyết định hợp đồng cho một hệ thống hay sản phẩm được tạo ra theo trình tự trong giai đoạn thực hiện hợp đồng phải:

e) Được tư vấn theo các thỏa thuận và phê duyệt theo nhà thiết kế và bên đảm bảo tính toàn vẹn và chấp thuận của chúng được tìm kiếm.

f) Đánh giá, nếu có thể thừa nhận bản chất trù định của bất kỳ yêu cầu nào cho nội dung của các tạo tác, thẩm quyền yêu cầu liên quan tới các đòi hỏi và yêu cầu mức toàn vẹn.

11.4 Tài liệu

Tài liệu đề cập tới:

a) Thỏa thuận hay phê duyệt một khía cạnh phải đi kèm với tài liệu của nó.

b) Tài liệu thỏa thuận, phê duyệt và các quyết định được tạo ra trong suốt quá trình đàm phán phải được phê duyệt bởi các bên đàm phán, đồng ý và/hoặc phê duyệt.

c) Tài liệu phải mô tả mối quan hệ của bên đảm bảo tính toàn vẹn, việc mở rộng độc lập của nhà sản xuất hệ thống hay sản phẩm và người đòi hỏi phù hợp với tiêu chuẩn này nếu người đòi hỏi không phải là nhà sản xuất.

Phụ lục A

(quy định)

Đầu ra và đầu vào cho khung mức toàn vẹn

A.1 Bảng của Điều 4 Khung mức toàn vẹn

Bảng A.1 - Đầu ra và đầu vào của các hoạt động trong Hình 1

Hoạt động xác định mức toàn vẹn	Đầu vào	Bước trung gian	Đầu ra
Xác định mức toàn vẹn hệ thống	• Danh sách thẩm quyền • Danh sách bên liên quan • Thông tin về hệ thống và môi trường • Yêu cầu bên liên quan • Vai trò của mức toàn vẹn trong vòng đời hệ thống	• Phân tích và đánh giá rủi ro • Gán mức toàn vẹn hệ thống	• Danh sách rủi ro • Phân loại rủi ro • Hệ quả tiêu cực, các điều kiện nguy hiểm và sự kiện bắt đầu cho mỗi rủi ro. • Các hạn chế cần thiết theo các điều kiện, sự xuất hiện và định thời của hệ quả • Danh sách giao diện hệ thống • Các hạn chế cần thiết theo hành vi hệ thống • Các đòi hỏi mức toàn vẹn • Mức toàn vẹn hệ thống
Xác định mức toàn vẹn phần tử	• Thông tin về hệ thống và môi trường. • Đòi hỏi mức toàn vẹn hệ thống.	• Phân tách hệ thống • Gán mức toàn vẹn hệ thống	• Danh sách phần tử hệ thống • Quan hệ phụ thuộc giữa các phần tử • Mức toàn vẹn phần tử
Đạt được yêu cầu mức toàn vẹn	• Thông tin về hệ thống và môi trường. • Tập phân định mức toàn vẹn cho mức toàn vẹn được sử dụng. • Yêu cầu mức toàn vẹn cho mỗi mức toàn vẹn được sử dụng.		• Bằng chứng của việc đạt được yêu cầu mức toàn vẹn cho tất cả phân định mức toàn vẹn. • Các đặc tả cho bất kỳ thay thế nào của yêu cầu mức toàn vẹn. • Các biện minh được văn bản hóa cho bất kỳ thay thế nào của yêu cầu mức toàn vẹn. • Bất kỳ phân tích liên quan nào.

Phụ lục B
(tham khảo)

Ví dụ sử dụng Tiêu chuẩn

B.1 Giới thiệu

Phụ lục này đưa ra phác thảo một ví dụ lý thuyết của việc định nghĩa và sử dụng mức toàn vẹn. Phụ lục này nhằm hỗ trợ việc hiểu cách sử dụng Tiêu chuẩn này.

B.2 Tổng quan

Ví dụ này xem xét các lĩnh vực của máy trả lời tự động (ATM) được sử dụng cho lĩnh vực ngân hàng. Trong ngữ cảnh này, một ATM cung cấp các dịch vụ cho tiền gửi và rút tiền mặt từ các tài khoản khách hàng mà không cần nhân viên thu ngân. Thông tin tài khoản được đặt tại máy chủ trung tâm và các máy ATM kết nối tới máy chủ thông qua một mạng để tham chiếu và thay đổi thông tin. Khi việc thỏa mãn khách hàng dựa trên việc hoạt động của các máy ATM và chúng được dùng thường xuyên khi các ngân hàng đóng cửa, khả năng sẵn có ở mức cao được yêu cầu. Hơn nữa, các máy ATM xử lý thông tin tài chính và cá nhân, độ tin cậy và an ninh mức cao cũng được yêu cầu. Để đơn giản hóa, các yêu cầu của một hệ thống ATM bao gồm bốn chức năng sau:

a) Một máy ATM có thể thực hiện gửi và rút tiền mặt từ các tài khoản khách hàng một cách chính xác.

b) Một máy ATM kết nối thành công với máy chủ trung tâm thông qua một mạng.

c) Một máy ATM cung cấp dịch vụ 24 giờ một ngày.

d) Không thông tin cá nhân nào được tiết lộ không đúng cách.

Nhằm hiểu nhu cầu, các tập đa mức của các mức toàn vẹn để phù hợp với các máy ATM được nhắm đến cho các người dùng khác nhau, xem xét hai loại máy ATM sau:

- Hệ thống X: một ATM chỉ xử lý một lượng nhỏ tiền mặt cho mỗi đơn vị giao dịch. Ví dụ: Các máy ATM được lắp đặt trong các trung tâm mua sắm hay sân bay để phục vụ khách hàng phổ thông.
- Hệ thống Y: một ATM xử lý một lượng lớn tiền mặt. Hệ thống này được giả định rằng các máy ATM này được lắp đặt ở các chi nhánh ngân hàng cho các khách hàng lớn.

Sự khác nhau trong các tình huống dẫn tới các mức rủi ro khác nhau.

CHÚ THÍCH Các tiêu chuẩn và hướng dẫn liên quan tới các máy ATM không được nêu ra trong ví dụ này theo lĩnh vực của các máy ATM được chọn như một điều tương tự cho độc giả. Mục đích của ví dụ này nhằm hỗ trợ đơn giản cho việc hiểu biết tiêu chuẩn này và không hiểu về lĩnh vực thực tế của việc phát triển và sử dụng máy ATM.

B.3 Định nghĩa mức toàn vẹn (Điều 6)

Đầu tiên, khung mức toàn vẹn tương ứng với Điều 6 “Định nghĩa các mức toàn vẹn”, được áp dụng cho lĩnh vực của hệ thống máy ATM. Khung mức toàn vẹn bao gồm ba mục sau:

- Nhãn mức toàn vẹn
- Đòi hỏi mức toàn vẹn
- Yêu cầu mức toàn vẹn

Bộ định danh của ví dụ các mức toàn vẹn cho các máy ATM được thể hiện trong Bảng B.1

Bảng B.1 - Ví dụ các mức toàn vẹn

Tính sẵn có	Độ tin cậy	An ninh
a	A	I
b	B	II
c	C	III

Một tập các mức toàn vẹn cho mỗi thuộc tính được yêu cầu cho hệ thống ATM. Mức toàn vẹn của một hệ thống tổng thể (ATM) là một phần tử của ILA x IIR x ILS trong đó ILA=(a,b,c), ILR=(A,B,C) và ILS=(I,II,III). Tiếp đó, một đòi hỏi mức toàn vẹn sẽ tương ứng với mỗi mức toàn vẹn. Chính xác, cho mỗi tập mức toàn vẹn, ví dụ: tính sẵn có, độ tin cậy và an ninh, một tập các đòi hỏi mức toàn vẹn sẽ tương ứng.

Bảng B.2 - Ví dụ dải giá trị thông thường của các đòi hỏi mức toàn vẹn

Mức toàn vẹn	*Đòi hỏi mức toàn vẹn*
a	MTTR được yêu cầu là một ngày hoặc ít hơn
b	MTTR được yêu cầu là một giờ hoặc ít hơn
c	MTTR được yêu cầu là 10 phút hoặc ít hơn
A	MTBF được yêu cầu là một tháng hoặc nhiều hơn
B	MTBF được yêu cầu là 6 tháng hoặc nhiều hơn
C	MTBF được yêu cầu là một năm hoặc nhiều hơn
I	EAL1 được yêu cầu hoặc cao hơn
II	EAL4 được yêu cầu hoặc cao hơn
III	EAL7 được yêu cầu

Trong Bảng B.2, MTTR nghĩa là *thời gian thực để sửa*, MTBF nghĩa là *thời gian thực giữa các lỗi* và EAL nghĩa là một *mức đảm bảo đánh giá* của lĩnh vực phổ biến cho việc đánh giá an ninh thông tin được định nghĩa trong ISO/IEC 15408. Cho mỗi đòi hỏi mức toàn vẹn, phạm vi áp dụng và độ không xác định cho phép được đưa ra như sau:

- Phạm vi áp dụng: các sản phẩm phần mềm được bao gồm trong thiết bị ATM, ví dụ: bất kỳ phần cứng và phần mềm nào trong máy chủ trung tâm được kết nối thông qua các mạng là ngoài phạm vi.
- Độ không xác định cho phép: 10% cho cả MTTR và MTBF, ví dụ: trong các thuật ngữ xác suất, xác suất 0.90 là các giá trị trong các phạm vi được đòi hỏi.

Danh sách yêu cầu mức toàn vẹn nằm trong Bảng B.3

Bảng B.3 - Ví dụ yêu cầu mức toàn vẹn và bằng chứng tương ứng

Mức toàn vẹn	*Yêu cầu mức toàn vẹn và bằng chứng tương ứng*
a	Thông tin lỗi được truy xuất Bằng chứng: đặc tả của chức năng ghi lại, tài liệu: kết quả thử nghiệm cho chức năng, việc thiết lập chức năng.
b	Bổ sung cho yêu cầu bên trên, chức năng mà các nhắc báo tự động thông tin lỗi cho nhà bảo trì Bằng chứng: đặc tả của hệ thống nhắc báo tự động, tài liệu: kết quả thử nghiệm cho chức năng, việc thiết lập chức năng.
c	Bổ sung cho yêu cầu bên trên, một vài hệ thống chịu lỗi phải được đính kèm Bằng chứng: đặc tả của hệ thống chịu lỗi, kết quả thử nghiệm, việc thiết lập
A	Lập kế hoạch, triển khai thử nghiệm và đánh giá cho cả việc thiết kế và thiết lập Bằng chứng: tài liệu: kết quả thử nghiệm và đánh giá
B	Bổ sung cho yêu cầu bên trên, việc thiết kế theo ngôn ngữ đặc tả hình thức Bằng chứng: tài liệu hoặc thiết kế được viết theo ngôn ngữ đặc tả hình thức.
C	Bổ sung cho yêu cầu bên trên, việc thiết lập phải được chứng minh hình thứcn nhằm thể hiện rằng nó thỏa mãn đặc tả Bằng chứng: tài liệu chứng minh
I	Tuân theo các hoạt động được xây dựng trong EAL1
II	Tuân theo các hoạt động được xây dựng trong EAL4
III	Tuân theo các hoạt động được xây dựng trong EAL7

Kết quả của Điều 6 phải bao gồm các biện minh yêu cầu mức toàn vẹn, ví dụ: một bày tỏ rằng mỗi yêu cầu mức toàn vẹn tương ứng là một điều kiện phù hợp cho đòi hỏi mức toàn vẹn tương ứng. Trong khi sự ngắn gọn của ví dụ lý thuyết này dẫn tới việc bỏ qua các biện minh này, chúng là yêu cầu thiết yếu của tiêu chuẩn này.

B.4 Sử dụng khung mức toàn vẹn (Điều 7 và 8)

Trong mục phụ này, một quy trình nhằm xác định một mức toàn vẹn cho một máy ATM sử dụng khung mức toàn vẹn của một máy ATM được định nghĩa trong mục phụ trước đó đã được thể hiện. Theo mục phụ của Điều 8.1, quy trình bắt đầu với việc định nghĩa một *tính toán tiêu chí rủi ro* cho việc đánh giá hệ thống. Giả định đầu tiên là một tình huống mà một ngân hàng A cung cấp các dịch vụ thông qua các

hệ thống ATM của cả loại X và Y. Lý tưởng hơn, tầm quan trọng của các rủi ro cho ngân hàng A được đánh giá bởi, ví dụ: việc kết hợp của ba khía cạnh sau:

(1) Phá hủy cơ sở vật chất: phá hủy bất kỳ cơ sở vật chất nào bao gồm chính hệ thống ATM đó.

(2) Tổn hại do sự bồi thường thất thoát của khách hàng: tổn hại bởi sự bồi thường thất thoát của tài khoản khách hàng do bất kỳ lỗi phần mềm hay sự rò rỉ thông tin cá nhân nào của máy ATM.

(3) Tổn hại danh tiếng ngân hàng: tổn hại danh tiếng do bất kỳ tai nạn nào, ví dụ: do một lỗi hệ thống

Khi khó khăn để xử lý và nhấn mạnh các đo lường trực tiếp bên trên, trong ví dụ này, nó được giả định rằng cách thức tính toàn các giá trị theo các đo lường bên trên từ các tác động sau cho mỗi rủi ro đã được thiết lập.

(i) Tầm quan trọng của khách hàng do tài khoản bị ảnh hưởng bởi hệ quả tiêu cực tương ứng (ví dụ: một tai nạn do một rủi ro)

(ii) Thời gian phục hồi của hệ quả tiêu cực tương ứng

(iii) Tần suất của hệ quả tiêu cực tương ứng

(iv) Tính minh bạch cho hệ quả tiêu cực tương ứng

Nhằm đơn giản hóa, chỉ *các rủi ro* sau cho phần mềm ATM được xem xét:

- Các vấn đề mạng không mong muốn
- Các tấn công nguy hại
- Các lỗi trong xử lý dữ liệu

Cho mỗi rủi ro, *các hệ quả tiêu cực* được minh họa bên dưới:

- Vấn đề mạng không mong muốn: Hãy xem xét hai trường hợp: kết nối mạng bị phá vỡ và một vài dữ liệu được bao gồm trong một máy ATM bị phá hủy bởi sự phá vỡ các kết nối. Trường hợp đầu do một vài lỗi dịch vụ của máy ATM nên khả năng sẵn có có liên quan. Trường hợp sau có thể do các lỗi thông tin trong giao dịch và có thể ảnh hưởng tới độ tin cậy.
- Các tấn công nguy hại: Khi tấn công nguy hại có thể dẫn tới việc rò rỉ thông tin cá nhân và cũng điều chỉnh dữ liệu tài khoản, khi đó an ninh và độ tin cậy được liên quan.
- Các lỗi trong việc xử lý dữ liệu: Khi một lỗi xử lý dữ liệu có thể gây ra một lỗi giao dịch thông tin, độ tin cậy là liên quan.

Các rủi ro hệ thống được phân tích dẫn đến các yêu cầu liên quan cho phần mềm.

Dựa trên việc phân tích nêu trên, *các hạn chế được yêu cầu* cho phần mềm theo mỗi loại ATM có thể được mô tả như sau.

Trường hợp của Hệ thống X: (1) Các dịch vụ ATM có thể bị ngắt phụ thuộc các vấn đề mạng không mong muốn hoặc các lý do khác. Loại ATM này được mong đợi cho việc sử dụng thường xuyên bởi các khách hàng phổ thông nên việc phục hồi trong hai ngày là hợp lý. (2) Các sai sót liên quan tới thông tin giao dịch cũng khả thi. Tuy nhiên, khi giới hạn lượng tiền mặt cho

mỗi giao dịch được thiết lập một giá trị thấp, thậm chí nếu một sai sót phát sinh và ngân hàng trả bồi hoàn cho giao dịch sai sót mà không vì lí do gì, tổn thất của nhân hàng vẫn thấp. Do đó, có MTBF là sáu tháng là hợp lý. (3) Các tấn công nguy hại có thể thỏa hiệp an ninh dẫn tới thông tin cá nhân có thể bị rò rỉ. Mặc dù mỗi giao dịch xử lý một lượng nhỏ tiền mặt, lượng tài khoản khách hàng và lượng thông tin nhạy cảm là lớn. Như một hệ quả, các hoạt động và bằng chứng EAL7 tương ứng được yêu cầu.

Trường hợp của Hệ thống Y: (1) Các dịch vụ ATM có thể bị ngắt. Khi người dùng tiềm năng của loại ATM là các khách hàng lớn, các lỗi dịch vụ lớn hơn mười phút có thể dẫn tới việc phá hủy nghiêm trọng cho khách hàng và các mối quan hệ của ngân hàng với họ và do vậy phải được phòng tránh. (2) Các vấn đề mạng với việc phá hủy dữ liệu và sai sót xử lý thông tin có thể dẫn tới các sai sót thông tin giao dịch. Lượng giao dịch của loại ATM này có thể lớn và do đó MTBF được đòi hỏi ít nhất là một năm. (3) An ninh cũng được yêu cầu mức đảm bảo chặt chẽ nhất.

Dựa trên các giới hạn được được yêu cầu nêu trên, mức toàn vẹn của mỗi loại hệ thống có thể được xác định tuân theo:

- Mức toàn vẹn của hệ thống X: (a, B, III)
- Mức toàn vẹn của hệ thống Y: (c, C, III)

Các mức toàn vẹn có thể được sử dụng không chỉ bởi các nhà đặt hàng máy ATM, mà còn bởi các người khách hàng có kiến thức hay người dùng máy ATM nhằm đưa ra các quyết định liên quan tới ngân hàng nào đặt tài khoản. Một người dùng có thể thu thập thông tin về các rủi ro của các máy ATM.

Nói chung, một hệ thống có một vài giao diện và các mức toàn vẹn có thể tương ứng cho mỗi giao diện riêng lẻ. Trong trường hợp này, bộ phận mạng của máy chủ trung tâm và giao diện người dùng đồ họa cho người dùng là hai ví dụ về giao diện. Do bản chất của các rủi ro trong trường hợp này, tất cả các giao diện của máy ATM được xem xét để gán cho cùng mức toàn vẹn

B.5 Mức toàn vẹn phần tử hệ thống (Điều 9)

Được thiết lập tập tập mức toàn vẹn của các giao diện, hệ thống đáng quan tâm phải được phân tách khi mỗi phần tử hệ thống (hoặc các giao diện phần tử khác nhau) tương ứng với một mức toàn vẹn. Quy trình này được lặp lại. Trong khi Điều 9 có thể nêu ra một phần lợi ích đáng kể được rút ra từ tiêu chuẩn này, chi tiết hóa một thiết kế nhiều mức cho các ATM và việc gán các mức toàn vẹn tương ứng với các phần tử hệ thống vượt ra ngoài phạm vi của ví dụ này.

B.6 Sử dụng mức toàn vẹn dựa trên tiêu chuẩn này

Ví dụ này minh họa một vài đặc trưng của việc sử dụng các mức toàn vẹn và lợi ích của chúng.

a) Lợi ích đầu tiên là các mức toàn vẹn có thể là một phương tiện kết nối các rủi ro của các hệ thống giữa các bên liên quan. Dựa trên các mức toàn vẹn tương ứng, bên liên quan có thể thảo luận về quan hệ thỏa hiệp giữa các rủi ro, kinh phí và có thể quyết định một kinh phí tương ứng để tránh

hay giảm thiểu rủi ro. Như một hệ quả, việc phát triển hệ thống được mong đợi nhằm tránh các đầu tư không cần thiết.

b) Ví dụ này cũng thể hiện rằng khung mức toàn vẹn có thể được sử dụng chỉ vượt ra ngoài mức an toàn liên quan tới các đặc tính. Các mức toàn vẹn an toàn được sử dụng rộng rãi trong khi các mức khác thì không.

Mặc dù trong ví dụ này, các biện minh hàm ý của các yêu cầu mức toàn vẹn cho đòi hỏi mức toàn vẹn được thừa nhận, có một đặc trưng quan trọng cho việc đưa ra các quyết định chắc chắn về hệ thống bởi các bên liên quan tương ứng.

Thư mục tài liệu tham khảo

[1] IEC 300-3-9, Risk Analysis of Technological Systems

[2] IEC 60300, Dependability management (nhiều phần)

[3] IEC 60812:2006, Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)

[4] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems (nhiều phần)

[5] IEC 61511:2003, Functional safety - Safety instrumented systems for the process industry sector (ba phần)

[6] IEC 61882, Hazard and operability studies (HAZOP studies) - Application guide

[7] IEEE Std 1012-2004, IEEE Standard for Software Verification and Validation

[8] ISO 13849, Safety of machinery - Safety-related parts of control systems (tất cả các phần)

[9] ISO 14620, Space systems - Safety requirements (tất cả các phần)

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

[11] ISO/IEC 15289:2006, Systems and software engineering - Content of systems and software life cycle process information products (Tài liệu)

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

[13] ISO/IEC 15504, Information technology - Process assessment (tất cả các phần)

[14] ISO/IEC 16085:2006, Systems and software engineering - Life cycle processes - Risk management

[15] ISO/TR 18152:2010, Ergonomics of human-system interaction - Specification for the process assessment of human-system issues

[16] ISO 19706:2007, Guidelines for assessing the fire threat to people

[17] ISO/IEC 19770, Information technology - Software asset management (tất cả các phần)

[18] ISO/IEC 21827, Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)

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

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

[21] ISO/IEC 27005, Information technology - Security techniques - Information security risk management

[22] ISO/IEC 42010:2007, Systems and software engineering - Recommended practice for architectural description of software-intensive systems