TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN IEC/ISO 31010:2013
IEC/ISO 31010:2009

Xuất bản lần 1

QUẢN LÝ RỦI RO – KỸ THUẬT ĐÁNH GIÁ RỦI RO

Risk management – Risk assessment techniques

HÀ NỘI - 2013

Mục lục

Lời nói đầu

TCVN IEC/ISO 31010:2013 hoàn toàn tương đương với IEC/ISO 31010:2009;

TCVN IEC/ISO 31010:2013 do Ban kỹ thuật tiêu chuẩn quốc gia TCVN/TC 176 *Quản lý chất lượng và đảm bảo chất lượng* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tổ chức ở mọi loại hình và quy mô đều đối mặt với những rủi ro có thể ảnh hưởng đến việc đạt được các mục tiêu của mình.

Những mục tiêu này có thể liên quan đến một phạm vi hoạt động của tổ chức, từ các sáng kiến chiến lược cho đến các hoạt động, quá trình và dự án của tổ chức và có thể được phản ánh trong các kết quả về mặt xã hội, môi trường, công nghệ, an toàn và an ninh, bằng các thước đo về thương mại, tài chính và kinh tế, cũng như các tác động xã hội, văn hóa, chính trị và uy tín

Tất cả hoạt động của tổ chức đều liên quan đến các rủi ro cần được quản lý. Quá trình quản lý rủi ro hỗ trợ cho việc ra quyết định bằng cách tính đến sự không chắc chắn và khả năng xảy ra của các sự kiện hoặc tình huống trong tương lai (được dự kiến hoặc không được dự kiến) và các tác động của chúng tới mục tiêu đã thống nhất.

Quản lý rủi ro bao gồm việc áp dụng các phương pháp hợp lý và hệ thống nhằm:

- trao đổi thông tin và tham vấn trong toàn bộ quá trình này;
- thiết lập bối cảnh để nhận diện, phân tích, định mức, xử lý rủi ro liên quan đến mọi hoạt động, quá trình, chức năng hoặc sản phẩm;
- theo dõi và xem xét rủi ro;
- báo cáo và ghi nhận các kết quả một cách thích hợp.

Đánh giá rủi ro là một phần trong quản lý rủi ro, đưa ra một quá trình có cấu trúc để xác định cách thức các mục tiêu có thể bị ảnh hưởng và phân tích rủi ro về các hệ quả và khả năng xảy ra các hệ quả trước khi quyết định có cần xử lý tiếp hay không.

Đánh giá độ rủi ro cố gắng trả lời các câu hỏi cơ bản sau đây:

- điều gì có thể xảy ra và tại sao (thông qua việc nhận diện rủi ro)?
- các hệ quả là gì?
- khả năng xảy ra các hệ quả trong tương lai là gì?
- có yếu tố nào làm giảm nhẹ hệ quả của rủi ro hoặc giảm khả năng xảy ra của rủi ro hay không?
- mức rủi ro có thể chịu đựng hoặc có thể chấp nhận được hay không và có cần xử lý tiếp hay không?

Tiêu chuẩn này nhằm phản ánh thực hành tốt hiện nay trong việc lựa chọn và vận dụng các kỹ thuật đánh giá rủi ro và không đề cập đến các khái niệm mới hoặc đang hình thành mà không đạt được mức độ thỏa mãn về sự đồng thuận chuyên môn.

Về bản chất tiêu chuẩn này mang tính tổng quan, vì vậy nó có thể đưa ra hướng dẫn cho nhiều ngành công nghiệp và nhiều loại hệ thống. Có thể có những tiêu chuẩn cụ thể hơn trong các ngành công nghiệp, thiết lập phương pháp luận và mức độ đánh giá ưu tiên cho các ứng dụng cụ thể. Nếu những tiêu chuẩn đó được hài hòa với tiêu chuẩn này, thì những tiêu chuẩn cụ thể đó nhìn chung là đầy đủ.

Quản lý rủi ro – Kỹ thuật đánh giá rủi ro

Risk management — Risk assessment techniques

1 Phạm vi áp dụng

Tiêu chuẩn này là một tiêu chuẩn hỗ trợ cho TCVN ISO 31000 và đưa ra hướng dẫn về việc lựa chọn và áp dụng kỹ thuật đánh giá rủi ro một cách hệ thống.

Việc đánh giá rủi ro được thực hiện theo tiêu chuẩn này sẽ đóng góp cho các hoạt động quản lý rủi ro khác.

Việc áp dụng các kỹ thuật được giới thiệu cùng sự viện dẫn các tiêu chuẩn khác trong đó khái niệm và việc áp dụng các kỹ thuật được mô tả chi tiết lớn hơn.

Tiêu chuẩn này không nhằm mục đích chứng nhận, quy định hay hợp đồng.

Tiêu chuẩn này không đưa ra tiêu chí cụ thể cho việc nhận biết nhu cầu phân tích rủi ro, cũng không quy định loại hình phương pháp phân tích rủi ro cần thiết cho một ứng dụng cụ thể.

Tiêu chuẩn này không đề cập đến tất cả các kỹ thuật và những kỹ thuật không nêu trong tiêu chuẩn này không có nghĩa là nó không hợp lý. Trên thực tế, một phương pháp có thể áp dụng với một tình huống cụ thể không có nghĩa là nhất thiết phải áp dụng phương pháp này.

CHÚ THÍCH: Tiêu chuẩn này không giải quyết một cách cụ thể vấn đề an toàn. Đây là một tiêu chuẩn chung về quản lý rủi ro và mọi sự viện dẫn đến vấn đề an toàn chỉ thuần túy mang tính chất tham khảo. Hướng dẫn về việc đưa các khía cạnh an toàn vào tiêu chuẩn được đưa ra trong TCVN 6844 (ISO/IEC Guide 51).

2 Tài liệu viện dẫn

Các tài liệu viện dẫn dưới đây rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng bản mới nhất, bao gồm cả các sửa đổi.

TCVN 9788 (ISO/IEC Guide 73), Quản lý rủi ro – Từ vựng.

TCVN ISO 31000 (ISO 31000), Quản lý rủi ro – Nguyên tắc và hướng dẫn.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ, định nghĩa trong TCVN 9788 (ISO/IEC Guide 73).

4 Các khái niệm đánh giá rủi ro

4.1 Mục đích và lợi ích

Mục đích của đánh giá rủi ro là đưa ra thông tin dựa trên bằng chứng và phân tích để ra quyết định đúng đắn về cách thức xử lý những rủi ro cụ thể và cách thức chọn các phương án khác nhau.

Một số lợi ích chủ yếu của việc đánh giá rủi ro là:

- hiểu rõ rủi ro và tác động tiềm ẩn của rủi ro tới các mục tiêu;
- cung cấp thông tin cho người ra quyết định;
- góp phần hiểu rõ rủi ro để hỗ trợ lựa chọn các phương án xử lý rủi ro;
- nhận biết những thành tố của rủi ro và những liên kết lỏng lẻo trong hệ thống và tổ chức;
- so sánh những rủi ro trong các hệ thống, công nghệ hoặc cách tiếp cận khác;
- trao đổi thông tin về rủi ro và sự không chắc chắn;
- hỗ trợ và thiết lập thứ tự ưu tiên;
- góp phần ngăn ngừa sự cố dựa trên việc điều tra sau sự cố;
- lựa chọn các hình thức xử lý rủi ro khác nhau;
- đáp ứng các yêu cầu chế định;
- cung cấp thông tin giúp đánh giá xem có nên chấp nhận rủi ro khi so sánh với tiêu chí đã được xác định;
- đánh giá những rủi ro đối với việc hủy bỏ khi kết thúc vòng đời.

4.2 Đánh giá rủi ro và khuôn khổ quản lý rủi ro

Tiêu chuẩn này giả định rằng việc đánh giá rủi ro được thực hiện trong khuôn khổ và quá trình quản lý rủi ro được mô tả trong TCVN ISO 31000.

Một khuôn khổ quản lý rủi ro đưa ra chính sách, thủ tục và các sắp đặt về tổ chức sẽ được áp dụng trong quản lý rủi ro ở tất cả các cấp của tổ chức.

Là một phần của khuôn khổ này, tổ chức cần có chính sách hoặc chiến lược để quyết định thời gian và cách thức những rủi ro cần được đánh giá.

Cụ thể, tổ chức thực hiện đánh giá rủi ro cần có sự rõ ràng về

- bối cảnh và mục tiêu của tổ chức;
- mức độ và loại rủi ro có thể chấp nhận được và cách thức xử lý những rủi ro không thể chấp nhận được;
- cách thức tích hợp đánh giá rủi ro vào các quá trình của tổ chức;

- các phương pháp và kỹ thuật được sử dụng để đánh giá rủi ro và đóng góp của những phương pháp và kỹ thuật này đối với quá trình quản lý rủi ro;
- trách nhiệm giải trình, trách nhiệm và quyền hạn thực hiện đánh giá rủi ro;
- các nguồn lực sẵn có để thực hiện đánh giá rủi ro;
- cách thức đánh giá rủi ro sẽ được báo cáo và xem xét.

4.3 Đánh giá rủi ro và quá trình quản lý rủi ro

4.3.1 Khái quát

Đánh giá rủi ro bao gồm các yếu tố cốt lõi của quá trình quản lý rủi ro được xác định trong TCVN ISO 31000 (ISO 31000) và bao gồm các yếu tố sau đây:

- trao đổi thông tin và tham vấn;
- thiết lập bối cảnh;
- đánh giá rủi ro (bao gồm nhận diện rủi ro, phân tích rủi ro và định mức rủi ro);
- xử lý rủi ro;
- theo dõi và xem xét.

Đánh giá rủi ro không phải là một hoạt động độc lập và phải được tích hợp đầy đủ vào các thành phần khác trong quá trình quản lý rủi ro.

4.3.2 Trao đổi thông tin và tham vấn

Thành công của đánh giá rủi ro phụ thuộc vào trao đổi thông tin và tham vấn một cách có hiệu lực với các bên liên quan.

Các bên liên quan tham gia vào quá trình quản lý rủi ro sẽ hỗ trợ trong việc:

- xây dựng kế hoạch trao đổi thông tin;
- xác định bối cảnh phù hợp;
- đảm bảo rằng lợi ích của các bên liên quan được hiểu rõ và được xem xét;
- tập hợp kiến thức chuyên môn trong các lĩnh vực khác nhau để nhận biết và phân tích rủi ro;
- đảm bảo rằng các quan điểm khác nhau được xem xét một cách thích hợp trong việc định mức rủi ro;
- đảm bảo rằng những rủi ro được nhận diện đầy đủ;
- đảm bảo sự xác nhận và hỗ trợ kế hoạch xử lý.

Các bên liên quan cần đóng góp vào giao diện của các quá trình đánh giá rủi ro và các nguyên tắc quản lý khác, bao gồm quản lý sự thay đổi, quản lý dự án và chương trình cũng như quản lý tài chính.

4.3.3 Thiết lập bối cảnh

Thiết lập bối cảnh xác định các thông số cơ bản cho quản lý rủi ro và lập ra phạm vi, tiêu chí cho phần còn lại của quá trình. Thiết lập bối cảnh bao gồm việc xem xét các thông số nội bộ và bên ngoài liên quan đến toàn bộ tổ chức, cũng như nền tảng để đánh giá những rủi ro.

Khi thiết lập bối cảnh, các mục tiêu đánh giá rủi ro, tiêu chí rủi ro và chương trình đánh giá rủi ro được xác định và được thống nhất.

Đối với một đánh giá rủi ro cụ thể, việc thiết lập bối cảnh cần bao gồm xác định bối cảnh nội bộ, bên ngoài và bối cảnh quản lý rủi ro và sự phân loại tiêu chí rủi ro:

a) Thiết lập bối cảnh bên ngoài đòi hỏi việc tạo sự quen thuộc với môi trường trong đó tổ chức và hệ thống hoạt động bao gồm:
   - các yếu tố văn hóa, chính trị, pháp lý, chế định, tài chính, kinh tế và môi trường cạnh tranh ở cấp quốc tế, quốc gia, khu vực hay địa phương;
   - các yếu tố định hướng và các xu hướng chính có tác động đến các mục tiêu của tổ chức; và
   - sự cảm nhận và giá trị của các bên liên quan bên ngoài.

b) Thiết lập bối cảnh nội bộ đòi hỏi sự hiểu biết về:
   - khả năng của tổ chức về các nguồn lực và kiến thức;
   - dòng thông tin và quá trình ra quyết định;
   - các bên liên quan nội bộ;
   - các mục tiêu và chiến lược đặt ra để đạt được mục tiêu;
   - cảm nhận, giá trị và văn hóa;
   - các chính sách và quá trình;
   - các tiêu chuẩn và mô hình chuẩn được tổ chức chấp nhận, và
   - các cấu trúc (ví dụ sự điều hành, vai trò và trách nhiệm giải trình).

c) Thiết lập bối cảnh quá trình quản lý rủi ro bao gồm:
   - xác định trách nhiệm giải trình và trách nhiệm;
   - xác định mức độ thực hiện các hoạt động quản lý rủi ro, những nội dung bao hàm và các loại trừ cụ thể;
   - xác định mức độ của dự án, quá trình, chức năng hoặc hoạt động về thời gian và địa điểm;

- xác định mối quan hệ giữa một dự án hoặc hoạt động cụ thể với các dự án hoặc hoạt động khác của tổ chức;
- xác định phương pháp luận đánh giá rủi ro;
- xác định tiêu chí rủi ro;
- xác định cách thức đánh giá việc thực hiện quản lý rủi ro;
- nhận biết và quy định các quyết định và các hành động phải được thực hiện, và
- nhận biết phạm vi hoặc lập khuôn khổ nghiên cứu cần thiết, mức độ của nghiên cứu, các mục tiêu và nguồn lực cần thiết cho việc nghiên cứu.

d) Xác định tiêu chí rủi ro liên quan đến việc quyết định

- tính chất và loại hệ quả được tính đến và cách thức đo lường các hệ quả;
- cách thức biểu diễn xác suất;
- cách thức xác định mức rủi ro;
- tiêu chí quyết định khi nào một rủi ro cần xử lý;
- tiêu chí quyết định khi nào một rủi ro có thể chấp nhận được và/hoặc có thể gánh chịu;
- sự kết hợp các rủi ro có được tính đến hay không và cách thức kết hợp các rủi ro sẽ được tính đến;

Tiêu chí có thể được dựa trên các nguồn như:

- các mục tiêu của quá trình được thống nhất;
- tiêu chí được nhận biết trong các quy định;
- nguồn dữ liệu chung;
- tiêu chí được chấp nhận chung trong ngành như mức độ an toàn tuyệt đối;
- sở thích rủi ro của tổ chức;
- các yêu cầu pháp lý và các yêu cầu khác đối với thiết bị hoặc các ứng dụng cụ thể.

4.3.4 Đánh giá rủi ro

Đánh giá rủi ro là quá trình tổng thể bao gồm nhận diện rủi ro, phân tích rủi ro và định mức rủi ro.

Các rủi ro có thể được đánh giá ở cấp độ tổ chức, cấp độ phòng ban, dự án, hoạt động riêng lẻ hoặc rủi ro cụ thể. Công cụ và kỹ thuật khác nhau có thể thích hợp trong các bối cảnh khác nhau.

Đánh giá rủi ro đưa ra hiểu biết về các rủi ro, nguyên nhân của rủi ro, hệ quả và xác suất của chúng. Điều này cung cấp thông tin cho các quyết định về việc:

- có nên thực hiện hoạt động hay không;

- cách thức để tối đa hóa các cơ hội;
- rủi ro có cần được xử lý hay không;
- lựa chọn những phương án với các rủi ro khác nhau;
- thiết lập thứ tự ưu tiên cho các phương án xử lý rủi ro;
- lựa chọn các chiến lược xử lý rủi ro thích hợp nhất sẽ mang lại những rủi ro bất lợi ở mức có thể gánh chịu.

4.3.5 Xử lý rủi ro

Việc đánh giá rủi ro, xử lý rủi ro hoàn chỉnh đòi hỏi lựa chọn và thống nhất một hoặc nhiều phương án phù hợp để thay đổi xác suất xảy ra, ảnh hưởng của rủi ro hoặc cả hai và thực hiện những phương án này.

Điều này được tiếp nối bởi một quá trình đánh giá lại theo chu kỳ mức rủi ro mới, với quan điểm xác định khả năng gánh chịu rủi ro theo tiêu chí thiết lập trước đó, để quyết định có cần xử lý thêm hay không.

4.3.6 Theo dõi và xem xét

Là một phần của quá trình quản lý rủi ro, rủi ro và các kiểm soát cần được theo dõi và xem xét một cách thường xuyên để kiểm tra xác nhận rằng

- những giả định về những rủi ro vẫn còn giá trị;
- những giả định làm cơ sở cho đánh giá rủi ro, vẫn còn giá trị bao gồm bối cảnh bên ngoài và nội bộ;
- các kết quả dự kiến đang đạt được;
- các kết quả đánh giá rủi ro phù hợp với kinh nghiệm thực tế;
- kỹ thuật đánh giá rủi ro đang được áp dụng một cách thích hợp;
- xử lý rủi ro có hiệu lực.

Trách nhiệm giải trình đối với việc theo dõi và thực hiện xem xét cần được thiết lập.

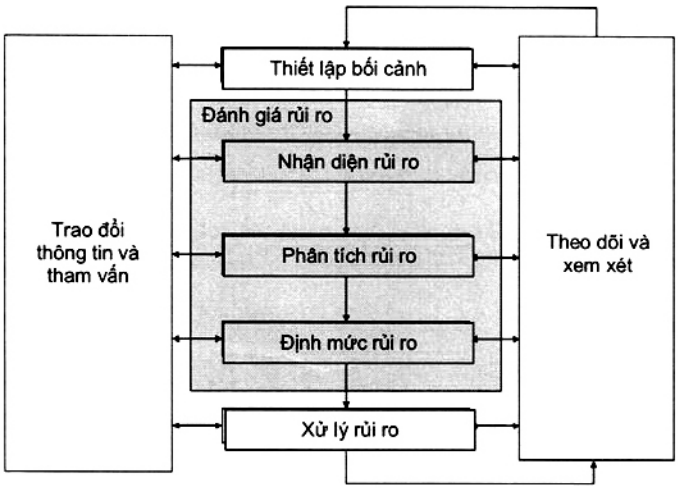
5 Quá trình đánh giá rủi ro

5.1 Khái quát

Đánh giá rủi ro cung cấp cho người ra quyết định và các bên chịu trách nhiệm sự hiểu biết cao hơn về rủi ro có thể ảnh hưởng đến việc đạt được các mục tiêu, sự thỏa đáng và hiệu lực của các kiểm soát đã thực hiện. Điều này mang lại cơ sở cho các quyết định về cách tiếp cận thích hợp nhất được sử dụng để xử lý những rủi ro. Đầu ra của đánh giá rủi ro là đầu vào cho quá trình ra quyết định của tổ chức.

Đánh giá rủi ro là một quá trình tổng thể gồm nhận diện rủi ro, phân tích rủi ro và định mức rủi ro (xem Hình 1). Cách thức áp dụng quá trình này không chỉ phụ thuộc vào bối cảnh quá trình quản lý rủi ro mà còn phụ thuộc vào phương pháp và kỹ thuật sử dụng để thực hiện việc định mức rủi ro.

Đánh giá rủi ro có thể yêu cầu một cách tiếp cận đa lĩnh vực vì các rủi ro có thể bao trùm hàng loạt các nguyên nhân và hệ quả.



Hình 1 – Đóng góp của đánh giá rủi ro vào quá trình quản lý rủi ro

5.2 Nhận diện rủi ro

Nhận diện rủi ro là quá trình tìm kiếm, thừa nhận và ghi lại các rủi ro.

Mục đích của nhận diện rủi ro là nhận biết những gì có thể xảy ra hoặc tình huống nào có thể tồn tại có thể ảnh hưởng đến việc đạt được các mục tiêu của hệ thống hoặc tổ chức. Khi một rủi ro được nhận diện, tổ chức cần nhận biết mọi kiểm soát hiện có như các tính năng thiết kế, con người, các quá trình và hệ thống.

Quá trình nhận diện rủi ro bao gồm việc nhận biết các nguyên nhân và nguồn rủi ro (mối nguy trong bối cảnh tác hại vật chất), các sự kiện, các tình huống hoặc các trường hợp có thể có tác động vật chất tới mục tiêu và tính chất của tác động đó.

Các phương pháp nhận diện rủi ro có thể bao gồm:

- các phương pháp dựa trên bằng chứng, ví dụ về các phương pháp này là danh mục kiểm tra và xem xét dữ liệu quá khứ;
- cách tiếp cận có hệ thống theo nhóm, trong đó một nhóm chuyên gia tuân theo một quá trình hệ thống để nhận diện rủi ro thông qua một bộ hướng dẫn hoặc câu hỏi được kết cấu;
- kỹ thuật suy luận quy nạp như HAZOP.

Có thể sử dụng các kỹ thuật hỗ trợ khác nhau để nâng cao độ chính xác và hoàn chỉnh trong việc nhận

diện rủi ro, bao gồm cả động não tập thể và phương pháp luận Delphi.

Dù kỹ thuật thực tế được vận dụng là gì, thì điều quan trọng là đưa ra sự thừa nhận về các yếu tố con người và tổ chức khi nhận diện rủi ro. Do đó, các yếu tố con người và tổ chức chệch khỏi dự kiến cần nằm trong quá trình nhận diện rủi ro cũng như các sự kiện "phần cứng" hoặc "phần mềm".

5.3 Phân tích rủi ro

5.3.1 Khái quát

Phân tích rủi ro là tạo dựng hiểu biết về rủi ro. Nó cung cấp đầu vào cho đánh giá rủi ro và cho quyết định về việc rủi ro có cần được xử lý hay không, về các chiến lược và phương pháp xử lý phù hợp nhất.

Phân tích rủi ro bao gồm việc xác định hệ quả và xác suất của chúng về các sự kiện rủi ro được nhận diện, có tính đến sự có mặt (hoặc không) và hiệu lực của bất kỳ sự kiểm soát hiện có nào. Sau đó hệ quả và xác suất của chúng được kết hợp để xác định một mức rủi ro.

Phân tích rủi ro đòi hỏi xem xét các nguyên nhân và nguồn rủi ro, hệ quả của chúng và xác suất hệ quả đó có thể xảy ra. Các yếu tố ảnh hưởng đến hệ quả và xác suất cần được nhận biết. Một sự kiện có thể có nhiều hệ quả và có thể ảnh hưởng đến nhiều mục tiêu. Các kiểm soát rủi ro hiện tại và hiệu lực của chúng cần được tính đến. Các phương pháp khác nhau đối với những phân tích này được mô tả trong Phụ lục B. Có thể cần nhiều kỹ thuật đối với các ứng dụng phức tạp.

Phân tích rủi ro thường bao gồm một ước lượng phạm vi các hệ quả tiềm ẩn có thể nảy sinh từ một sự kiện, tình huống hoặc trường hợp và xác suất kết hợp của chúng để đo mức rủi ro. Tuy nhiên trong một số trường hợp, như khi hệ quả dường như là không đáng kể hoặc xác suất được dự kiến là rất thấp, ước lượng tham số duy nhất có thể đủ để ra quyết định thực hiện.

Trong một số trường hợp, một hệ quả có thể xảy ra như là kết quả của hàng loạt các sự kiện hoặc điều kiện khác nhau hoặc khi sự kiện cụ thể không được nhận biết. Trong trường hợp này, trọng tâm của đánh giá rủi ro là phân tích tầm quan trọng và điểm yếu của các thành tố trong hệ thống nhằm xác định việc xử lý liên quan đến các mức bảo vệ hoặc phục hồi chiến lược.

Các phương pháp được sử dụng trong phân tích rủi ro có thể là định tính, bán định lượng hoặc định lượng. Mức độ chi tiết cần thiết phụ thuộc vào ứng dụng cụ thể, sự sẵn có của dữ liệu đáng tin cậy và các nhu cầu ra quyết định của tổ chức. Một số phương pháp và mức độ chi tiết của phân tích có thể do luật pháp quy định.

Đánh giá định tính xác định hệ quả, xác suất và mức rủi ro bằng các mức như "cao", "trung bình" và "thấp", có thể kết hợp hệ quả và xác suất và đánh giá mức rủi ro theo các tiêu chí định tính.

Phương pháp bán định lượng sử dụng thang chia bằng số đối với hệ quả và xác suất kết hợp chúng để đưa ra một mức rủi ro bằng cách sử dụng công thức. Thang đo có thể là tuyến tính hoặc thang logarit, hay có mối quan hệ khác nào đó, công thức được sử dụng cũng có thể khác nhau.

Phân tích định lượng ước tính giá trị thực tế đối với hệ quả và xác suất của chúng, và đưa ra giá trị về mức rủi ro theo các đơn vị cụ thể được xác định khi thiết lập bối cảnh. Phân tích định lượng đầy đủ không phải luôn có thể thực hiện hoặc được mong muốn do thông tin về hệ thống hoặc hoạt động được phân tích chưa đầy đủ, thiếu dữ liệu, ảnh hưởng bởi các yếu tố con người, v.v...hay do nỗ lực phân tích định lượng không được đảm bảo hoặc được yêu cầu. Trong trường hợp như vậy, việc xếp hạng tương đối định tính hoặc bán định lượng rủi ro của các chuyên gia có kiến thức về những lĩnh vực riêng của họ vẫn có thể có hiệu lực.

Trong các trường hợp phân tích định tính, cần diễn giải rõ tất cả các điều kiện được sử dụng và cơ sở cho tất cả các tiêu chí cần được ghi nhận lại.

Ngay cả khi sự lượng hóa đầy đủ được thực hiện, vẫn cần thừa nhận rằng các mức rủi ro được tính toán là các ước lượng. Cần thận trọng để đảm bảo rằng chúng không được ấn định độ chính xác và độ chụm không nhất quán với độ chính xác của dữ liệu và phương pháp được sử dụng.

Các mức rủi ro cần được thể hiện ở dạng phù hợp nhất với loại rủi ro đó và hỗ trợ việc định mức rủi ro. Trong một số trường hợp, mức rủi ro có thể được thể hiện theo một phân bố xác suất đối với nhiều hệ quả.

5.3.2 Đánh giá kiểm soát

Mức rủi ro sẽ phụ thuộc vào sự thỏa đáng và hiệu lực của các kiểm soát hiện có. Các câu hỏi cần được giải quyết bao gồm:

- các kiểm soát hiện có đối với một rủi ro cụ thể là gì?
- các kiểm soát đó có khả năng xử lý rủi ro một cách thỏa đáng để rủi ro được kiểm soát ở mức có thể gánh chịu không?
- trên thực tế, các kiểm soát có hoạt động theo cách thức dự kiến không và chúng có thể được chứng tỏ là có hiệu lực khi cần không?

Những câu hỏi này chỉ có thể được trả lời với sự tin cậy khi sẵn có tài liệu và các quá trình đảm bảo.

Mức độ hiệu lực đối với kiểm soát cụ thể, hoặc sự phù hợp của các kiểm soát liên quan, có thể được thể hiện định tính, bán định lượng hoặc định lượng. Trong hầu hết các trường hợp, độ chính xác cao không được đảm bảo. Tuy nhiên, có thể có ý nghĩa khi thể hiện và ghi nhận một thước đo hiệu lực của kiểm soát rủi ro để có thể thực hiện đánh giá xem nỗ lực được sử dụng tốt nhất hay chưa trong việc cải thiện một kiểm soát hoặc đưa ra cách xử lý rủi ro khác.

5.3.3 Phân tích hệ quả

Phân tích hệ quả xác định tính chất và loại hình tác động có thể xảy ra, giả định rằng một tình huống hoặc các trường hợp sự kiện cụ thể đã xảy ra. Một sự kiện có thể có một loạt các tác động với các mức độ khác nhau và ảnh hưởng tới một loạt các mục tiêu và các bên liên quan khác nhau. Loại hệ quả được phân tích và các bên liên quan bị ảnh hưởng sẽ được quyết định khi bối cảnh được thiết lập.

Phân tích hệ quả có thể thay đổi từ một mô tả đơn giản về các kết quả đến mô hình hóa định lượng chi tiết phân tích điểm yếu.

Các tác động có thể có hệ quả thấp nhưng xác suất cao, hệ quả cao và xác suất thấp, hay một kết quả trung gian nào đó. Trong một số trường hợp, nên tập trung vào các rủi ro với các kết quả tiềm ẩn rất lớn, vì những rủi ro này thường là mối quan tâm lớn nhất của các nhà quản lý. Trong những trường hợp khác, có thể quan trọng khi phân tích cả các rủi ro với hệ quả cao và thấp một cách riêng biệt. Ví dụ, một vấn đề thường xuyên nhưng tác động thấp (hoặc đã thành thói quen) có thể có tác động tích lũy lớn hoặc lâu dài. Ngoài ra, các hành động xử lý để giải quyết hai loại hình rủi ro khác biệt này thường là khá khác nhau, vì vậy sẽ hữu ích khi phân tích chúng một cách riêng biệt.

Phân tích hệ quả có thể bao gồm:

- đưa vào xem xét các kiểm soát hiện có để xử lý các hệ quả, cùng với tất cả các yếu tố đóng góp liên quan có tác động đến hệ quả;
- liên kết các hệ quả của rủi ro với các mục tiêu ban đầu;
- xem xét cả hệ quả tức thời và những hệ quả có thể phát sinh sau một thời gian nhất định, nếu điều này phù hợp với phạm vi đánh giá;
- xem xét hệ quả thứ phát, như những hệ quả tác động tới các hệ thống, hoạt động, thiết bị hoặc tổ chức liên quan.

5.3.4 Phân tích khả năng xảy ra và ước lượng xác suất

Ba cách tiếp cận chung thường được sử dụng để ước lượng xác suất; chúng có thể được sử dụng riêng lẻ hoặc kết hợp:

a) Việc sử dụng dữ liệu lịch sử liên quan để nhận biết các sự kiện hoặc tình huống đã xảy ra trong quá khứ và từ đó có thể ngoại suy xác suất xảy ra của chúng trong tương lai. Dữ liệu được sử dụng cần phù hợp với loại hình hệ thống, thiết bị, tổ chức hoặc hoạt động được xem xét cũng như tiêu chuẩn hoạt động liên quan của tổ chức. Nếu trước đó tần suất xảy ra rất thấp, thì mọi ước lượng về xác suất sẽ rất không chắc chắn. Điều này áp dụng đặc biệt đối với sự cố không xảy ra, khi không thể giả định sự kiện, tình huống hoặc trường hợp sẽ không xảy ra trong tương lai.

b) Dự báo xác suất bằng cách sử dụng kỹ thuật dự đoán như phân tích cây lỗi và phân tích cây sự kiện (xem Phụ lục B). Khi dữ liệu quá khứ không sẵn có hoặc không đầy đủ, cần suy ra xác suất bằng cách phân tích hệ thống, hoạt động, thiết bị hoặc tổ chức và tình trạng thành công hay thất bại liên quan của tổ chức. Sau đó, dữ liệu số về thiết bị, con người, tổ chức và hệ thống có được từ kinh nghiệm hoạt động hoặc nguồn dữ liệu được công bố được kết hợp để đưa ra ước lượng xác suất của sự kiện đầu. Khi sử dụng kỹ thuật dự đoán, quan trọng là đảm bảo có được sự xem xét cần thiết trong phân tích xác suất về phương thức sai lỗi chung bao gồm sai lỗi ngẫu nhiên của một số bộ phận hoặc thành phần khác nhau trong hệ thống nảy sinh từ cùng một nguyên nhân. Có thể cần kỹ thuật mô phỏng để tạo ra xác suất của sai lỗi về thiết bị và cấu trúc do sự lão hóa và quá trình xuống cấp, bằng việc tính toán các tác động của sự không chắc chắn.

c) Ý kiến chuyên gia có thể được sử dụng trong một quá trình có hệ thống và kết cấu để ước lượng xác suất. Đánh giá của chuyên gia cần được dựa trên tất cả thông tin sẵn có liên quan bao gồm thông tin quá khứ, hệ thống cụ thể, tổ chức cụ thể, thực nghiệm, thiết kế, v.v... Có một số phương pháp chính thức để suy luận đánh giá của chuyên gia trong đó đưa ra sự hỗ trợ cho việc xây dựng các câu hỏi thích hợp. Các phương pháp sẵn có bao gồm cách tiếp cận Delphi, so sánh theo cặp, phân loại và các đánh giá xác suất tuyệt đối.

5.3.5 Phân tích sơ bộ

Các rủi ro có thể được phân loại để nhận diện những rủi ro quan trọng nhất hoặc để loại trừ những rủi ro không đáng kể hoặc ít quan trọng hơn từ phân tích sâu hơn. Mục đích là để đảm bảo các nguồn lực sẽ được tập trung vào những rủi ro quan trọng nhất. Cần thận trọng để không loại ra những rủi ro thấp nhưng xảy ra thường xuyên và có một tác động tổng hợp đáng kể.

Việc phân loại cần dựa trên tiêu chí được xác định theo bối cảnh. Phân tích sơ bộ xác định một hoặc nhiều chuỗi hành động sau đây:

- quyết định xử lý các rủi ro mà không cần đánh giá thêm;
- bác bỏ những rủi ro không quan trọng mà không đánh giá việc xử lý;
- tiến tới đánh giá rủi ro chi tiết hơn.

Các giả định và các kết quả ban đầu cần được lập thành văn bản.

5.3.6 Độ không đảm bảo và độ nhạy

Thường có độ không đảm bảo đáng kể liên quan đến phân tích rủi ro. Cần sự hiểu biết về độ không đảm bảo để diễn giải và trao đổi thông tin về các kết quả phân tích rủi ro một cách hiệu lực. Phân tích độ không đảm bảo kèm theo dữ liệu, phương pháp và mô hình sử dụng để nhận diện và phân tích rủi ro đóng góp một phần quan trọng trong việc áp dụng chúng. Phân tích độ không đảm bảo đòi hỏi việc xác định độ biến động hoặc sự thiếu chính xác trong kết quả, do độ biến động chung trong các tham số và các giả định được sử dụng để xác định các kết quả. Một lĩnh vực liên quan nhiều đến phân tích sự không chắc chắn là phân tích độ nhạy.

Phân tích độ nhạy đòi hỏi xác định quy mô và mức độ quan trọng của rủi ro đối với sự thay đổi các thông số đầu vào riêng lẻ. Phân tích này được sử dụng để nhận biết những dữ liệu yêu cầu chính xác và những dữ liệu kém nhạy hơn và do đó ít tác động tới độ chính xác tổng thể.

Sự hoàn chỉnh và chính xác của phân tích rủi ro cần được nêu đầy đủ nhất có thể. Các nguồn không đảm bảo cần được nhận biết khi có thể và cần đề cập đến cả độ không đảm bảo của dữ liệu và mô hình/phương pháp. Các thông số theo đó phân tích tính nhạy và độ nhạy cần được nêu rõ.

5.4 Định mức rủi ro

Định mức rủi ro đòi hỏi so sánh các mức rủi ro ước lượng với tiêu chí rủi ro xác định khi bối cảnh được thiết lập, để xác định tầm quan trọng của mức và loại hình rủi ro.

Định mức rủi ro vận dụng hiểu biết có được về rủi ro từ quá trình phân tích rủi ro để ra quyết định về các hành động tương lai. Các xem xét về đạo đức, pháp lý, tài chính và xem xét khác gồm cả cảm nhận về rủi ro, cũng là các đầu vào cho quyết định.

Các quyết định có thể bao gồm:

- rủi ro có cần xử lý hay không;
- thứ tự ưu tiên xử lý;
- có cần thực hiện hành động hay không;
- lộ trình nào cần tuân theo.

Tính chất của các quyết định cần được đưa ra và tiêu chí được sử dụng để ra quyết định được xác định khi thiết lập bối cảnh nhưng chúng cần phải được xem xét lại chi tiết hơn ở giai đoạn này khi đã biết rõ hơn về những rủi ro cụ thể đã được nhận diện.

Khuôn khổ đơn giản nhất để xác định tiêu chí rủi ro là một mức duy nhất phân chia các rủi ro cần xử lý khỏi những rủi ro không cần xử lý. Điều này đưa ra các kết quả đơn giản một cách hấp dẫn nhưng không phản ánh sự không chắc chắn liên quan đến cả việc ước lượng rủi ro và xác định ranh giới giữa những rủi ro cần xử lý và rủi ro không cần xử lý.

Quyết định về việc có xử lý hay không và cách thức xử lý rủi ro có thể phụ thuộc vào chi phí và lợi ích của việc tiếp nhận rủi ro cũng như các chi phí và lợi ích của việc thực hiện những kiểm soát được cải tiến.

Một cách tiếp cận phổ biến nhằm phân chia rủi ro thành ba nhóm:

a) nhóm cao hơn có mức rủi ro được coi là không thể gánh chịu bất kể lợi ích mà hoạt động có thể mang lại ra sao và việc xử lý rủi ro là thiết yếu bất kể chi phí xử lý thế nào;

b) nhóm trung bình (hoặc vùng "xám") trong đó chi phí và lợi ích được tính đến và các cơ hội được cân bằng với các hệ quả tiềm ẩn;

c) nhóm thấp hơn có mức rủi ro được coi là không đáng kể, hoặc quá nhỏ không cần biện pháp xử lý rủi ro nào.

Hệ thống tiêu chí 'thấp nhất có thể' hay ALARP[1] được sử dụng trong ứng dụng an toàn tuân theo cách tiếp cận này, trong đó, ở nhóm trung bình, có thang đo trượt đối với các rủi ro thấp khi chi phí và lợi ích có thể so sánh trực tiếp, trong khi đối với các rủi ro cao, khả năng gây hại phải được giảm, cho đến khi chi phí để giảm hoàn toàn không cân đối đối với lợi ích an toàn đạt được.

5.5 Tài liệu

Quá trình đánh giá rủi ro cần được lập thành văn bản cùng với các kết quả của việc đánh giá. Rủi ro cần được thể hiện bằng các thuật ngữ dễ hiểu và các đơn vị thể hiện mức rủi ro cần rõ ràng.

[1] ALARP: As low as reasonably practicable

Mức độ báo cáo sẽ phụ thuộc vào mục tiêu và phạm vi của việc đánh giá. Ngoại trừ các đánh giá đơn giản, tài liệu có thể bao gồm:

- mục tiêu và phạm vi;
- mô tả các phần liên quan của hệ thống và các chức năng của chúng;
- bản tóm tắt bối cảnh nội bộ và bên ngoài của tổ chức và bối cảnh đó liên quan thế nào tới tình huống, hệ thống hoặc các trường hợp được đánh giá;
- tiêu chí rủi ro được áp dụng và lý giải cho các tiêu chí đó;
- các hạn chế, giả định và lý giải cho các giả thuyết;
- phương pháp luận đánh giá;
- kết quả nhận diện rủi ro;
- dữ liệu, giả định, nguồn giả định và xác nhận giá trị của chúng;
- kết quả phân tích rủi ro và định mức rủi ro;
- phân tích độ nhạy và độ không đảm bảo;
- các giả định quan trọng và các yếu tố khác cần được theo dõi;
- thảo luận kết quả;
- các kết luận và khuyến nghị;
- tài liệu tham khảo.

Nếu việc đánh giá rủi ro hỗ trợ quá trình quản lý rủi ro một cách liên tục, thì việc đánh giá cần được thực hiện và lập thành văn bản theo cách có thể duy trì trong toàn bộ vòng đời của hệ thống, tổ chức, thiết bị hoặc hoạt động. Việc đánh giá cần được cập nhật khi thông tin mới quan trọng sẵn có và bối cảnh thay đổi, phù hợp với nhu cầu của quá trình quản lý.

5.6 Theo dõi và xem xét đánh giá rủi ro

Quá trình đánh giá rủi ro sẽ chú trọng vào bối cảnh và các yếu tố khác có thể thay đổi theo thời gian và có thể làm thay đổi hoặc làm mất ý nghĩa của việc đánh giá rủi ro. Những yếu tố này cần được nhận biết một cách cụ thể cho việc theo dõi và xem xét liên tục nhờ đó việc đánh giá rủi ro có thể được cập nhật khi cần.

Dữ liệu được theo dõi để cải thiện đánh giá rủi ro cũng cần được nhận biết và được thu thập.

Hiệu lực của việc kiểm soát cũng cần được theo dõi và lập thành văn bản nhằm cung cấp dữ liệu để sử dụng trong phân tích rủi ro. Trách nhiệm giải trình cho việc lập và xem xét bằng chứng và tài liệu cần được xác định.

5.7 Áp dụng đánh giá rủi ro trong các giai đoạn của vòng đời

Nhiều hoạt động, dự án và sản phẩm có thể được xem xét vòng đời bắt đầu từ ý tưởng và việc xác định ban đầu cho tới việc hiện thực hóa hoàn chỉnh cuối cùng có thể bao gồm sự ngừng hoạt động và hủy bỏ phần cứng.

Đánh giá rủi ro có thể được áp dụng ở tất cả các giai đoạn của vòng đời và thường được áp dụng nhiều lần với các mức độ chi tiết khác nhau để hỗ trợ các quyết định cần được đưa ra ở từng giai đoạn.

Các giai đoạn của vòng đời có các yêu cầu khác nhau và cần các kỹ thuật khác nhau. Ví dụ, ở giai đoạn ý tưởng và xác định, khi một cơ hội được nhận biết, đánh giá rủi ro có thể được sử dụng để quyết định xem có tiếp tục hay không.

Khi sẵn có một số phương án, đánh giá rủi ro có thể được sử dụng để đánh giá các ý tưởng thay thế để hỗ trợ quyết định đưa ra sự cân bằng nhất giữa các rủi ro tích cực và tiêu cực.

Trong giai đoạn thiết kế và phát triển, đánh giá rủi ro góp phần

- đảm bảo rằng rủi ro hệ thống là có thể gánh chịu được,
- quá trình sàng lọc thiết kế,
- nghiên cứu hiệu quả của chi phí,
- nhận diện các rủi ro tác động tới giai đoạn tiếp theo của vòng đời.

Khi hoạt động được tiếp tục, đánh giá rủi ro có thể được sử dụng để cung cấp thông tin hỗ trợ trong việc xây dựng các quy trình cho các điều kiện bình thường và khẩn cấp.

6 Lựa chọn kỹ thuật đánh giá rủi ro

6.1 Khái quát

Điều này mô tả cách thức lựa chọn kỹ thuật đánh giá rủi ro. Các phụ lục liệt kê và giải thích chi tiết một loạt các công cụ và kỹ thuật có thể được sử dụng để thực hiện đánh giá rủi ro hoặc hỗ trợ quá trình đánh giá rủi ro. Đôi khi có thể cần áp dụng nhiều phương pháp đánh giá.

6.2 Lựa chọn kỹ thuật

Đánh giá rủi ro có thể được thực hiện ở các mức độ sâu sắc và chi tiết khác nhau và sử dụng một hoặc nhiều phương pháp từ đơn giản đến phức tạp. Hình thức đánh giá và đầu ra của nó cần phù hợp với tiêu chí rủi ro được xây dựng như là một phần của việc thiết lập bối cảnh. Phụ lục A minh họa mối quan hệ khái niệm giữa các loại kỹ thuật đánh giá rủi ro được sử dụng rộng rãi và các yếu tố thể hiện trong một tình huống rủi ro đã biết và đưa ra các ví dụ minh hoạ về cách thức tổ chức có thể lựa chọn kỹ thuật đánh giá rủi ro thích hợp đối với một tình huống cụ thể.

Tóm lại, kỹ thuật phù hợp cần thể hiện các đặc trưng sau:

- xác đáng và phù hợp với tình huống hoặc tổ chức đang được xem xét;
- đưa ra các kết quả dưới hình thức nâng cao hiểu biết về tính chất của rủi ro và cách thức rủi ro có thể được xử lý;
- có khả năng sử dụng theo cách có thể theo dõi, lặp lại và kiểm tra xác nhận.

Cần đưa ra các lý do lựa chọn kỹ thuật về tính xác đáng và phù hợp. Khi tích hợp các kết quả từ những nghiên cứu khác nhau, kỹ thuật được sử dụng và các đầu ra cần có thể so sánh được.

Khi ra quyết định thực hiện một đánh giá rủi ro và xác định các mục tiêu và phạm vi, kỹ thuật cần được lựa chọn dựa trên các yếu tố thích hợp như:

- mục tiêu nghiên cứu. Các mục tiêu của đánh giá rủi ro sẽ có một ảnh hưởng trực tiếp vào các kỹ thuật sử dụng. Ví dụ, nếu thực hiện một nghiên cứu so sánh giữa các phương án khác nhau, có thể chấp nhận sử dụng các mô hình hệ quả ít chi tiết hơn cho các phần của hệ thống không bị ảnh hưởng bởi sự khác biệt;
- nhu cầu của người ra quyết định. Trong một số trường hợp, cần có mức độ chi tiết cao để ra một quyết định tốt, trong các trường hợp khác một sự hiểu biết tổng quát hơn là đủ;
- loại hình và phạm vi các rủi ro đang được phân tích;
- mức độ tiềm ẩn của các hệ quả. Quyết định về chiều sâu đánh giá rủi ro được thực hiện cần phản ánh cảm nhận ban đầu về những hệ quả (mặc dù điều này có thể phải được sửa đổi khi đánh giá sơ bộ được hoàn thiện);
- mức độ chuyên nghiệp, nguồn nhân lực và các nguồn lực cần thiết khác. Một phương pháp đơn giản nhưng được thực hiện tốt, có thể mang lại các kết quả tốt hơn một quy trình phức tạp nhưng được thực hiện kém, miễn là nó đáp ứng các mục tiêu và phạm vi của đánh giá. Thông thường, nỗ lực trong đánh giá cần phù hợp với mức rủi ro tiềm ẩn được phân tích;
- sự sẵn có của thông tin và dữ liệu. Một số kỹ thuật đòi hỏi nhiều thông tin và dữ liệu hơn những kỹ thuật khác;
- nhu cầu sửa đổi/cập nhật đánh giá rủi ro. Việc đánh giá có thể cần được sửa đổi/cập nhật trong tương lai và một số kỹ thuật có thể sửa đổi nhiều hơn kỹ thuật khác về mặt này;
- mọi yêu cầu chế định và hợp đồng.

Các yếu tố khác nhau ảnh hưởng đến việc lựa chọn cách tiếp cận đánh giá rủi ro như sự sẵn có của các nguồn lực, bản chất và độ không đảm bảo trong dữ liệu và thông tin sẵn có và sự phức tạp của việc áp dụng (xem Bảng A.2).

6.3 Sự sẵn có của các nguồn lực

Các nguồn lực và khả năng có thể ảnh hưởng đến việc lựa chọn kỹ thuật đánh giá rủi ro bao gồm:

- khả năng về các kỹ năng, kinh nghiệm và năng lực của nhóm đánh giá rủi ro;
- những ràng buộc về thời gian và các nguồn lực khác trong tổ chức;
- ngân sách sẵn có nếu các nguồn lực bên ngoài là cần thiết.

6.4 Bản chất của độ không đảm bảo và độ không đảm bảo

Bản chất của độ không đảm bảo và độ không đảm bảo đòi hỏi phải hiểu rõ chất lượng, số lượng và tính toàn vẹn của thông tin sẵn có liên quan đến rủi ro được xem xét. Điều này bao gồm mức độ thông tin đầy đủ về rủi ro, các nguồn lực và nguyên nhân của nó và hệ quả đối với việc đạt được các mục tiêu là sẵn có. Độ không đảm bảo có thể bắt nguồn từ chất lượng dữ liệu kém hoặc thiếu dữ liệu cần thiết và đáng tin cậy. Để minh họa, các phương pháp thu thập dữ liệu có thể thay đổi, cách thức tổ chức sử dụng các phương pháp như vậy có thể thay đổi hoặc tổ chức có thể không thực hiện phương pháp thu thập hoàn toàn hiệu lực để thu thập dữ liệu về rủi ro được nhận diện.

Độ không đảm bảo cũng có thể gắn với bối cảnh nội bộ và bên ngoài của tổ chức. Dữ liệu sẵn có không phải lúc nào cũng đưa ra cơ sở đáng tin cậy cho việc dự đoán tương lai. Đối với các loại rủi ro duy nhất, dữ liệu quá khứ có thể không sẵn có hoặc có thể có các diễn giải dữ liệu sẵn có khác nhau của các bên liên quan khác nhau. Những người thực hiện đánh giá rủi ro cần hiểu loại hình và bản chất của độ không đảm bảo và đánh giá cao các ẩn ý đối với độ tin cậy của các kết quả đánh giá rủi ro. Những điều này cần luôn luôn được trao đổi thông tin với người ra quyết định.

6.5 Sự phức tạp

Tự các rủi ro có thể đã phức tạp, ví dụ như trong các hệ thống phức tạp cần đánh giá rủi ro trong toàn hệ thống thay vì xử lý mỗi thành phần riêng biệt và bỏ qua sự tương tác. Trong một số trường hợp khác, xử lý một rủi ro duy nhất có thể có ý nghĩa ở một nơi nào khác và có thể tác động đến các hoạt động khác. Tác động do hệ quả và sự phụ thuộc rủi ro cần được tìm hiểu để đảm bảo rằng trong quản lý rủi ro không tạo ra một tình huống không thể gánh chịu ở nơi khác. Hiểu rõ sự phức tạp của một rủi ro duy nhất hoặc của một tập hợp các rủi ro trong một tổ chức là thiết yếu cho việc lựa chọn phương pháp hoặc kỹ thuật đánh giá rủi ro thích hợp.

6.6 Áp dụng đánh giá rủi ro trong các giai đoạn của vòng đời

Có thể coi nhiều hoạt động, dự án và sản phẩm có vòng đời bắt đầu từ ý tưởng và việc xác định ban đầu thông qua việc thực hiện tới sự hoàn thành cuối cùng và có thể bao gồm việc ngừng hoạt động và loại bỏ phần cứng.

Việc đánh giá rủi ro có thể được áp dụng ở tất cả các giai đoạn của vòng đời và thường được áp dụng nhiều lần với các mức độ chi tiết khác nhau để hỗ trợ các quyết định cần đưa ra ở mỗi giai đoạn.

Các giai đoạn của vòng đời có các nhu cầu khác nhau và yêu cầu các kỹ thuật khác nhau. Ví dụ, trong giai đoạn ý tưởng và xác định, khi một cơ hội được nhận biết, đánh giá rủi ro có thể được sử dụng để quyết định xem có triển khai tiếp hay không.

Nếu sẵn có một số phương án, đánh giá rủi ro có thể được sử dụng để đánh giá các ý tưởng thay thế giúp quyết định điều gì mang lại sự cân bằng rủi ro tốt nhất.

Trong giai đoạn thiết kế và phát triển, đánh giá rủi ro góp phần vào

- đảm bảo các rủi ro hệ thống có thể gánh chịu được,
- quá trình sàng lọc thiết kế,
- nghiên cứu hiệu quả của chi phí,
- nhận diện các rủi ro tác động tới các giai đoạn của vòng đời tiếp theo.

Khi tiếp tục hoạt động, đánh giá rủi ro có thể được sử dụng để cung cấp thông tin hỗ trợ xây dựng các quy trình đối với các điều kiện thông thường và khẩn cấp.

6.7 Các loại kỹ thuật đánh giá rủi ro

Kỹ thuật đánh giá rủi ro có thể được phân loại theo nhiều cách khác nhau để hỗ trợ việc hiểu các điểm mạnh và điểm yếu liên quan của chúng. Các bảng trong Phụ lục A nêu tương quan một số kỹ thuật tiềm ẩn và các loại kỹ thuật với mục đích minh họa.

Mỗi kỹ thuật được xây dựng thêm trong Phụ lục B theo tính chất của đánh giá mà kỹ thuật đó cung cấp và hướng dẫn về khả năng áp dụng các kỹ thuật đối với các tình huống nhất định.

Phụ lục A
(tham khảo)

So sánh các kỹ thuật đánh giá rủi ro

A.1 Các loại kỹ thuật

Việc phân loại đầu tiên cho thấy cách thức các kỹ thuật áp dụng cho từng bước của quá trình đánh giá rủi ro như sau:

- nhận diện rủi ro;
- phân tích rủi ro – phân tích hệ quả;
- phân tích rủi ro – định tính, bán định lượng hoặc ước lượng xác suất định lượng;
- phân tích rủi ro – đánh giá hiệu lực của mọi kiểm soát hiện có;
- phân tích rủi ro – ước lượng mức rủi ro;
- định mức rủi ro.

Đối với mỗi bước trong quá trình đánh giá rủi ro việc áp dụng phương pháp được mô tả là khả năng áp dụng cao, áp dụng hoặc không áp dụng được (xem Bảng A.1).

A.2 Các yếu tố ảnh hưởng đến việc lựa chọn kỹ thuật đánh giá rủi ro

Tiếp theo là các thuộc tính của các phương pháp được mô tả về:

- sự phức tạp của vấn đề và các phương pháp cần thiết để phân tích,
- bản chất độ không đảm bảo và độ không đảm bảo của đánh giá rủi ro dựa trên lượng thông tin sẵn có và những điều cần thiết để thỏa mãn các mục tiêu;
- mức độ các nguồn lực cần thiết về thời gian và mức độ chuyên môn, các nhu cầu dữ liệu hoặc chi phí,
- phương pháp có thể cung cấp một đầu ra định lượng hay không.

Các ví dụ về loại phương pháp đánh giá rủi ro sẵn có được liệt kê trong Bảng A.2 trong đó mỗi phương pháp được đánh giá là cao, trung bình hoặc thấp theo những thuộc tính này.

Bảng A.1 – Khả năng áp dụng các công cụ sử dụng trong đánh giá rủi ro

Các công cụ và kỹ thuật	Quá trình đánh giá rủi ro					Xem Phụ lục
	Nhận diện rủi ro	Phân tích rủi ro			Định mức rủi ro	
		Hệ quả	Xác suất	Mức rủi ro		
Động não tập thể	SA[1)]	NA[2)]	NA	NA	NA	B 01
Phỏng vấn có cấu trúc hoặc bán cấu trúc	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Danh mục kiểm tra	SA	NA	NA	NA	NA	B 04
Phân tích mối nguy ban đầu	SA	NA	NA	NA	NA	B 05
Nghiên cứu mối nguy và khả năng vận hành (HAZOP)	SA	SA	A[3)]	A	A	B 06
Phân tích mối nguy và điểm kiểm soát trọng yếu (HACCP)	SA	SA	NA	NA	SA	B 07
Đánh giá rủi ro môi trường	SA	SA	SA	SA	SA	B 08
Cấu trúc "Điều gì - nếu?" (SWIFT)	SA	SA	SA	SA	SA	B 09
Phân tích kịch bản	SA	SA	A	A	A	B 10
Phân tích tác động kinh doanh	A	SA	A	A	A	B 11
Phân tích nguyên nhân gốc rễ	NA	SA	SA	SA	SA	B 12
Phân tích phương thức và tác động sai lỗi	SA	SA	SA	SA	SA	B 13
Phân tích cây lỗi	A	NA	SA	A	A	B 14
Phân tích cây sự kiện	A	SA	A	A	NA	B 15
Phân tích nguyên nhân và hệ quả	A	SA	SA	A	A	B 16
Phân tích nguyên nhân và tác động	SA	SA	NA	NA	NA	B 17
Phân tích bảo vệ theo lớp (LOPA)	A	SA	A	A	NA	B 18
Cây quyết định	NA	SA	SA	A	A	B 19
Phân tích độ tin cậy của con người	SA	SA	SA	SA	A	B 20
Phân tích hình nơ bướm	NA	A	SA	SA	A	B 21
Bảo trì tập trung vào sự tin cậy	SA	SA	SA	SA	SA	B 22
Phân tích mạch ẩn	A	NA	NA	NA	NA	B 23
Phân tích Markov	A	SA	NA	NA	NA	B 24
Mô phỏng Monte Carlo	NA	NA	NA	NA	SA	B 25
Thống kê Bayes và mạng Bayes	NA	SA	NA	NA	SA	B 26
Đường FN	A	SA	SA	A	SA	B 27
Chỉ số rủi ro	A	SA	SA	A	SA	B 28
Ma trận hệ quả/xác suất	SA	SA	SA	SA	A	B 29
Phân tích chi phí/ lợi ích	A	SA	A	A	A	B 30
Phân tích quyết định đa tiêu chí (MCDA)	A	SA	A	SA	A	B 31

[1)] SA (Strongly applicable) :Khả năng áp dụng cao

[2)] NA (not applicable): Không áp dụng được

[3)] A (Applicable): Áp dụng

Bảng A.2 – Các thuộc tính của việc lựa chọn công cụ đánh giá rủi ro

Loại kỹ thuật đánh giá độ rủi ro	Mô tả	Sự liên quan của các yếu tố ảnh hưởng			Có thể cung cấp đầu ra định lượng
		Nguồn lực và khả năng	Bản chất độ không đảm bảo và độ không đảm bảo	Sự phức tạp	
PHƯƠNG PHÁP TÌM KIẾM					
Danh mục kiểm tra	Một hình thức nhận diện rủi ro đơn giản. Kỹ thuật đưa ra danh mục về sự không chắc chắn điển hình cần được xem xét. Người sử dụng tham khảo danh mục được xây dựng trước đó, các quy phạm hoặc tiêu chuẩn.	Thấp	Thấp	Thấp	Không
Phân tích sơ bộ mối nguy	Một phương pháp phân tích quy nạp đơn giản, mục tiêu của nó là nhận biết những tình huống và sự kiện nguy hiểm và nguy hại có thể gây ra cho một hoạt động, thiết bị hoặc hệ thống nhất định.	Thấp	Cao	Trung bình	Không
PHƯƠNG PHÁP HỖ TRỢ					
Phỏng vấn và động não tập thể có cấu trúc	Phương tiện thu thập tập hợp lớn các ý tưởng và việc đánh giá, phân loại chúng của nhóm. Động não tập thể có thể được khuyến khích bằng những nhắc nhở hoặc bởi kỹ thuật phỏng vấn một người với một người và một người với nhiều người	Thấp	Thấp	Thấp	Không
Kỹ thuật Delphi	Một cách thức kết hợp các quan điểm của chuyên gia có thể hỗ trợ việc nhận biết nguồn và ảnh hưởng, ước lượng xác suất và hệ quả và định	Trung bình	Trung bình	Trung bình	Không

Loại kỹ thuật đánh giá độ rủi ro	Mô tả	Sự liên quan của các yếu tố ảnh hưởng			Có thể cung cấp đầu ra định lượng
		Nguồn lực và khả năng	Bản chất độ không đảm bảo và độ không đảm bảo	Sự phức tạp	
	mức rủi ro. Đây là một kỹ thuật cộng tác để xây dựng sự đồng thuận giữa các chuyên gia. Đòi hỏi phân tích độc lập và bỏ phiếu của các chuyên gia.				
Cấu trúc SWIFT "Điều gì – nếu"	Một hệ thống thúc đẩy nhóm nhận diện các rủi ro. Thường được sử dụng trong một hội thảo có sự hỗ trợ. Thường được liên kết với kỹ thuật phân tích và kỹ thuật định mức rủi ro.	Trung bình	Trung bình	Bất kỳ	Không
Phân tích độ tin cậy của con người (HRA)	Đánh giá độ tin cậy của con người (HRA) liên quan đến tác động của con người tới việc thực hiện hệ thống và có thể được sử dụng để đánh giá những ảnh hưởng của sai lỗi của con người tới hệ thống.	Trung bình	Trung bình	Trung bình	Có
PHÂN TÍCH KỊCH BẢN					
Phân tích nguyên nhân gốc rễ (phân tích tổn thất duy nhất)	Tổn thất duy nhất đã xảy ra được phân tích để tìm hiểu các nguyên nhân và cách thức hệ thống hoặc quá trình có thể được cải tiến để tránh những tổn thất này trong tương lai. Việc phân tích phải xem xét những kiểm soát nào được đặt ra tại thời điểm xảy ra tổn thất và cách thức những kiểm soát có thể được cải tiến.	Trung bình	Thấp	Trung bình	Không
Phân tích kịch bản	Các tình huống có thể xảy ra trong tương lai được nhận biết thông qua tưởng tượng hoặc ngoại suy từ hiện tại và những rủi ro khác được xem	Trung bình	Cao	Trung bình	

Loại kỹ thuật đánh giá độ rủi ro	Mô tả	Sự liên quan của các yếu tố ảnh hưởng			Có thể cung cấp đầu ra định lượng
		Nguồn lực và khả năng	Bản chất độ không đảm bảo và độ không đảm bảo	Sự phức tạp	
	xét bằng việc giả định từng tình huống có thể xảy ra. Điều này có thể được thực hiện chính thức hoặc không chính thức một cách định tính hoặc định lượng.				Không
Đánh giá tính độc hại của rủi ro	Nhận biết, phân tích các mối nguy, nhận biết các lộ trình theo đó mục tiêu quy định có thể hứng chịu mối nguy. Thông tin về mức độ hứng chịu và tính chất của tác hại gây ra bởi mức độ hứng chịu được kết hợp để đưa ra thước đo xác suất mà tác hại quy định sẽ xảy ra.	Cao	Cao	Trung bình	Có
Phân tích tác động kinh doanh	Đưa ra phân tích về cách thức những rủi ro gián đoạn chính có thể tác động đến các hoạt động của một tổ chức và nhận biết, lượng hóa khả năng cần thiết để quản lý tác động đó.	Trung bình	Trung bình	Trung bình	Không
Phân tích cây lỗi	Kỹ thuật bắt đầu với sự kiện không mong muốn (sự kiện đầu) và xác định tất cả các cách biến cố có thể xảy ra. Những điều này được biểu diễn bằng đồ thị trong một sơ đồ hình cây hợp lý. Khi cây lỗi đã được xây dựng, cần đưa ra xem xét về cách thức giảm hoặc loại bỏ các nguyên nhân/nguồn tiềm ẩn.	Cao	Cao	Trung bình	Có

Loại kỹ thuật đánh giá độ rủi ro	Mô tả	Sự liên quan của các yếu tố ảnh hưởng			Có thể cung cấp đầu ra định lượng
		Nguồn lực và khả năng	Bản chất độ không đảm bảo và độ không đảm bảo	Sự phức tạp	
Phân tích cây sự kiện	Sử dụng lập luận quy nạp để chuyển xác suất về các sự kiện khởi đầu khác nhau thành các đầu ra có thể.	Trung bình	Trung bình	Trung bình	Có
Phân tích nguyên nhân/ hệ quả	Sự kết hợp phân tích cây lỗi và cây sự kiện cho phép đưa vào sự chậm trễ về thời gian. Cả nguyên nhân và hệ quả của một sự kiện khởi đầu đều được xem xét.	Cao	Trung bình	Cao	Có
Phân tích nguyên nhân và tác động	Một tác động có thể có một số yếu tố đóng góp có thể được nhóm thành các loại khác nhau. Các yếu tố đóng góp thường được nhận biết thông qua động não tập thể và được thể hiện trong một cấu trúc hình cây hoặc biểu đồ xương cá	Thấp	Thấp	Trung bình	Không
PHÂN TÍCH CHỨC NĂNG					
FMEA và FMECA	FMEA (Phân tích tác động và phương thức sai lỗi) là một kỹ thuật nhận biết các phương thức và cơ chế sai lỗi và tác động của chúng. Có một số loại FMEA: FMEA thiết kế (hoặc sản phẩm) được sử dụng cho phụ tùng và sản phẩm, FMEA hệ thống được sử dụng cho các hệ thống, FMEA quá trình được sử dụng cho các quá trình sản xuất và lắp ráp, FMEA dịch vụ và FMEA phần mềm.	Trung bình	Trung bình	Trung bình	Có

Loại kỹ thuật đánh giá độ rủi ro	Mô tả	Sự liên quan của các yếu tố ảnh hưởng			Có thể cung cấp đầu ra định lượng
		Nguồn lực và khả năng	Bản chất độ không đảm bảo và độ không đảm bảo	Sự phức tạp	
	FMEA có thể được tiếp nối bằng một phân tích mức độ trọng yếu xác định tầm quan trọng của mỗi phương thức sai lỗi một cách định lượng, bán định lượng, hoặc định tính (FMECA). Phân tích mức độ trọng yếu có thể dựa trên xác suất mà phương thức sai lỗi sẽ gây ra sai lỗi hệ thống, hoặc mức rủi ro liên quan với phương thức sai lỗi, hoặc số lượng ưu tiên rủi ro.				
Bảo trì tập trung vào độ tin cậy	Một phương pháp nhận biết các chính sách cần được thực hiện để quản lý những sai lỗi nhằm đạt được một cách hiệu lực và hiệu quả sự an toàn cần thiết, sự sẵn có và tính kinh tế trong vận hành đối với tất cả các loại thiết bị	Trung bình	Trung bình	Trung bình	Có
Phân tích ẩn (Phân tích mạch ẩn)	Phương pháp luận cho việc nhận biết các lỗi thiết kế. Điều kiện ẩn là phần cứng, phần mềm tiềm ẩn, hoặc điều kiện kết hợp có thể gây ra một sự kiện không mong muốn xảy ra hoặc có thể ngăn chặn một sự kiện mong muốn và không do sai lỗi thành phần gây ra. Những điều kiện này được đặc trưng bởi tính chất ngẫu nhiên và khả năng tránh bị phát hiện trong thử nghiệm hệ thống được chuẩn hóa khắt khe nhất. Các điều kiện ẩn có thể gây ra hoạt động không đúng, mất tính sẵn sàng của hệ thống, sự	Trung bình	Trung bình	Trung bình	Không

Loại kỹ thuật đánh giá độ rủi ro	Mô tả	Sự liên quan của các yếu tố ảnh hưởng			Có thể cung cấp đầu ra định lượng
		Nguồn lực và khả năng	Bản chất độ không đảm bảo và độ không đảm bảo	Sự phức tạp	
	chậm trễ chương trình, hoặc thậm chí gây tử vong hoặc bị thương cho nhân sự.				
HAZOP Nghiên cứu mối nguy và khả năng vận hành	Quá trình nhận diện rủi ro chung để xác định cách chệch hướng có thể có khỏi việc thực hiện mong đợi được dự kiến. Nó sử dụng một từ chỉ dẫn dựa trên hệ thống. Các giá trị tới hạn của độ chệch được đánh giá	Trung bình	Cao	Cao	Không
HACCP Phân tích mối nguy và điểm kiểm soát trọng yếu	Một hệ thống có hệ thống, chủ động và phòng ngừa để đảm bảo chất lượng sản phẩm, độ tin cậy và sự an toàn của các quá trình bằng cách đo lường và theo dõi các đặc trưng cụ thể được yêu cầu nằm trong những giới hạn xác định	Trung bình	Trung bình	Trung bình	Không
ĐÁNH GIÁ VIỆC KIỂM SOÁT					
LOPA Phân tích bảo vệ theo lớp	(Cũng có thể được gọi là phân tích rào cản). Nó cho phép các kiểm soát và hiệu lực của chúng được đánh giá	Trung bình	Trung bình	Trung bình	Có

Loại kỹ thuật đánh giá độ rủi ro	Mô tả	Sự liên quan của các yếu tố ảnh hưởng			Có thể cung cấp đầu ra định lượng
		Nguồn lực và khả năng	Bản chất độ không đảm bảo và độ không đảm bảo	Sự phức tạp	
Phân tích hình nơ bướm	Một cách lập biểu đồ đơn giản mô tả và phân tích lộ trình của một rủi ro từ những mối nguy đến các đầu ra và xem xét các kiểm soát. Nó có thể được coi là một sự kết hợp hợp lý của phân tích cây lỗi nguyên nhân của một sự kiện (được hiển thị bởi nút thắt của nơ hình bướm) và phân tích cây sự kiện những hệ quả	Trung bình	Cao	Trung bình	Có
PHƯƠNG PHÁP THỐNG KÊ					
Phân tích Markov	Phân tích Markov, đôi khi được gọi là phân tích *trạng thái trống,* thường được sử dụng trong phân tích các hệ thống phức tạp có thể khôi phục lại mà có thể tồn tại ở nhiều trạng thái, bao gồm cả các trạng thái suy giảm khác nhau	Cao	Thấp	Cao	Có
Phân tích Monte-Carlo	Mô phỏng Monte Carlo được sử dụng để thiết lập độ biến động tổng hợp trong hệ thống do các biến động trong hệ thống gây ra, đối với một số đầu vào, trong đó mỗi đầu vào có phân bố xác định và các đầu vào liên quan đến đầu ra thông qua mối quan hệ xác định. Phân tích này có thể được sử dụng cho một mô hình cụ thể trong đó sự tương tác của các đầu vào khác nhau có thể được xác định bằng toán học. Đầu vào có thể dựa trên nhiều loại phân bố theo bản chất của độ không đảm bảo chúng được dự kiến đại	Cao	Thấp	Cao	Có

Loại kỹ thuật đánh giá độ rủi ro	Mô tả	Sự liên quan của các yếu tố ảnh hưởng			Có thể cung cấp đầu ra định lượng
		Nguồn lực và khả năng	Bản chất độ không đảm bảo và độ không đảm bảo	Sự phức tạp	
	diện. Để đánh giá rủi ro, phân bố tam giác hoặc phân bố beta thường được sử dụng				
Phân tích Bayes	Quy trình thống kê sử dụng dữ liệu phân bố đã biết để đánh giá xác suất của kết quả. Phân tích Bayes phụ thuộc vào độ chính xác của phân bố đã biết để suy ra một kết quả chính xác. Mạng lưới niềm tin của Bayes lập ra mô hình nguyên nhân và tác động trong một loạt các lĩnh vực bằng việc nắm bắt các mối quan hệ xác suất của các đầu vào biến đổi để rút ra kết quả.	Cao	Thấp	Cao	Có

Phụ lục B
(tham khảo)

Kỹ thuật đánh giá rủi ro

B.1 Động não tập thể

B.1 Tổng quan

Động não tập thể đòi hỏi việc kích thích và khuyến khích cuộc đàm luận theo dòng chảy tự do giữa một nhóm người có kiến thức để nhận biết các phương thức sai lỗi tiềm ẩn và các mối nguy, rủi ro, tiêu chí liên quan để quyết định và/hoặc các phương án cho việc xử lý. Thuật ngữ "động não tập thể" thường được sử dụng rất lỏng lẻo để nói về bất kỳ loại hình thảo luận nhóm nào. Tuy nhiên động não tập thể thực sự bao gồm các kỹ thuật cụ thể để cố gắng đảm bảo rằng trí tưởng tượng của con người do những suy nghĩ và tuyên bố của những người khác trong nhóm khơi dậy.

Việc hỗ trợ một cách hiệu lực là rất quan trọng trong kỹ thuật này và bao gồm sự khuyến khích của cuộc thảo luận ở thời điểm bắt đầu, sự thúc đẩy nhóm định kỳ vào các khu vực liên quan khác và nắm bắt các vấn đề phát sinh từ cuộc thảo luận (mà thường khá sôi nổi).

B.1.2 Sử dụng

Động não tập thể có thể được sử dụng cùng với các phương pháp đánh giá rủi ro khác được mô tả dưới đây hoặc có thể là một kỹ thuật độc lập để khuyến khích việc tư duy có tưởng tượng ở bất kỳ giai đoạn nào của quá trình quản lý rủi ro và vòng đời hệ thống. Nó có thể được sử dụng cho các cuộc thảo luận cấp cao ở đó các vấn đề được nhận biết, cho việc xem xét chi tiết hơn hoặc ở một mức độ chi tiết đối với các vấn đề cụ thể.

Động não tập thể nhấn mạnh đặc biệt vào trí tưởng tượng. Bởi vậy nó đặc biệt hữu ích khi nhận biết các rủi ro của công nghệ mới, khi không có dữ liệu hoặc khi các giải pháp mới đối với các vấn đề là cần thiết.

B.1.3 Đầu vào

Một nhóm người có kiến thức về tổ chức, hệ thống, quá trình hoặc ứng dụng đang được đánh giá.

B.1.4 Quá trình

Động não tập thể có thể chính thức hoặc không chính thức. Động não tập thể chính thức thường có cấu trúc hơn trong đó những người tham gia được chuẩn bị trước và buổi họp có mục đích và kết quả được xác định bằng việc đánh giá các ý tưởng đưa ra. Động não tập thể không chính thức ít được cấu trúc hơn và thường đặc biệt hơn.

Quá trình chính thức:

- người trợ giúp chuẩn bị những hướng dẫn và hoạt động tư duy thích hợp với bối cảnh trước cuộc họp;

- các mục tiêu của cuộc họp được xác định và các quy tắc được giải thích;
- người trợ giúp bắt đầu một chuỗi tư duy và mọi người khai thác các ý tưởng bằng cách nhận biết nhiều vấn đề nhất có thể. Tại thời điểm này không có thảo luận về việc sự vật nên hoặc không nên nằm trong một danh mục hoặc các tuyên bố cụ thể có ý nghĩa gì vì điều này sẽ hạn chế dòng suy nghĩ tự do. Tất cả đầu vào đều được chấp nhận và không có điều gì bị phê phán và nhóm tiến tới một cách nhanh chóng để cho phép các ý tưởng kích thích lối suy nghĩ một chiều.
- người trợ giúp có thể đưa mọi người sang một hướng mới khi một hướng tư duy đã cạn hoặc cuộc thảo luận chệch hướng quá xa. Tuy nhiên ý tưởng là thu thập càng nhiều ý tưởng khác nhau càng tốt cho phân tích sau đó.

B.1.5 Đầu ra

Các đầu ra phụ thuộc vào giai đoạn của quá trình quản lý rủi ro tại đó nó được áp dụng, ví dụ ở giai đoạn nhận diện, các đầu ra có thể là một danh mục các rủi ro và các kiểm soát hiện tại.

B.1.6 Điểm mạnh và hạn chế

Điểm mạnh của động não tập thể bao gồm:

- khuyến khích trí trưởng tượng giúp nhận biết những rủi ro và các giải pháp mới;
- lôi kéo các bên liên quan chính và do đó hỗ trợ toàn bộ quá trình trao đổi thông tin;
- tương đối nhanh chóng và dễ dàng thiết lập.

Những hạn chế bao gồm:

- những người tham gia có thể thiếu kỹ năng và kiến thức để đóng góp một cách hiệu lực;
- do không được cấu trúc một cách tương đối nên sẽ khó chứng tỏ rằng quá trình là toàn diện, ví dụ tất cả các rủi ro tiềm ẩn đã được nhận biết;
- có thể có các động lực nhóm cụ thể khi một số người với các ý tưởng có giá trị im lặng hoàn toàn trong khi những người khác chi phối cuộc thảo luận. Điều này có thể khắc phục bằng cách động não tập thể qua máy tính, sử dụng một diễn đàn trò chuyện hoặc kỹ thuật nhóm danh nghĩa. Động não tập thể qua máy tính có thể được thiết lập giấu tên, do đó tránh được các vấn đề cá nhân và chính trị có thể gây cản trở dòng ý tưởng tự do. Trong các kỹ thuật nhóm danh nghĩa các ý tưởng được đề xuất ẩn danh đến một người trung gian và sau đó được thảo luận theo nhóm.

B.2 Cuộc phỏng vấn có cấu trúc hoặc bán cấu trúc

B.2.1 Tổng quan

Trong một cuộc phỏng vấn có cấu trúc, người được phỏng vấn riêng lẻ được hỏi một bộ các câu hỏi được chuẩn bị từ một bảng nhắc nhở khuyến khích người được phỏng vấn nhìn nhận một tình huống từ một góc độ khác và từ đó nhận diện các rủi ro từ góc độ đó. Một cuộc phỏng vấn bán cấu trúc cũng

tương tự, nhưng cho phép trò chuyện tự do hơn để khai thác các vấn đề nảy sinh.

B.2.2 Sử dụng

Các cuộc phỏng vấn có cấu trúc và bán cấu trúc là hữu ích khi khó để tập hợp mọi người cùng tham gia một cuộc họp động não tập thể hoặc khi việc thảo luận tự do liên tục trong một nhóm không thích hợp đối với tình huống hoặc người liên quan. Chúng được sử dụng thường xuyên nhất để nhận biết các rủi ro hoặc để đánh giá hiệu lực của những kiểm soát hiện tại như một phần của phân tích rủi ro. Chúng có thể được áp dụng ở bất kỳ giai đoạn nào của một dự án hoặc quá trình. Chúng là phương tiện cung cấp đầu vào để đánh giá rủi ro cho các bên liên quan.

B.2.3 Đầu vào

Đầu vào bao gồm:

- xác định rõ các mục tiêu phỏng vấn;
- danh sách những người phỏng vấn được lựa chọn từ các bên liên quan phù hợp;
- một bộ các câu hỏi được chuẩn bị.

B.2.4 Quá trình

Một bộ câu hỏi liên quan được lập để hướng dẫn người phỏng vấn. Các câu hỏi cần có kết thúc mở khi có thể, cần đơn giản, bằng ngôn ngữ phù hợp với người được phỏng vấn và chỉ bao gồm một vấn đề. Có thể có các câu hỏi nối tiếp để làm rõ được chuẩn bị.

Sau đó các câu hỏi được đặt ra cho người được phỏng vấn. Khi tìm cách soạn thảo kỹ lưỡng, các câu hỏi cần có kết thúc mở. Cần thận trọng để không "dẫn dắt" người được phỏng vấn.

Các câu trả lời cần được xem xét ở một mức độ linh hoạt để đưa ra cơ hội khai thác các lĩnh vực người được phỏng vấn có thể muốn hướng tới.

B.2.5 Đầu ra

Đầu ra là quan điểm của các bên liên quan về các vấn đề là đối tượng của các cuộc phỏng vấn.

B.2.6 Điểm mạnh và hạn chế

Điểm mạnh của các cuộc phỏng vấn có cấu trúc là:

- cuộc phỏng vấn có cấu trúc cho phép mọi người có thời gian xem xét suy nghĩ về một vấn đề;
- trao đổi thông tin trực tiếp có thể cho phép xem xét các vấn đề sâu hơn;
- cuộc phỏng vấn có cấu trúc cho phép sự tham gia của một số lượng lớn các bên liên quan hơn so với động não tập thể sử dụng nhóm tương đối nhỏ;

Các hạn chế như sau:

- tốn nhiều thời gian của người trợ giúp để lấy được nhiều ý kiến theo cách này;
- cho phép sự chệch hướng và không loại bỏ khỏi thảo luận nhóm;
- có thể không đạt được sự kích thích trí tưởng tượng là một tính năng của động não tập thể.

B.3 Kỹ thuật Delphi

B.3.1 Tổng quan

Kỹ thuật Delphi là một quy trình đạt được sự đồng thuận đáng tin cậy về quan điểm của một nhóm chuyên gia. Mặc dù hiện nay thuật ngữ này thường được sử dụng rộng rãi để nói về bất kỳ hình thức nào của động não tập thể, thì một tính năng thiết yếu của kỹ thuật Delphi như được xây dựng ban đầu, là các chuyên gia bày tỏ quan điểm của mình một cách riêng rẽ và ẩn danh mà vẫn tiếp cận quan điểm của chuyên gia khác khi quá trình tiến triển.

B.3.2 Sử dụng

Kỹ thuật Delphi có thể được áp dụng ở giai đoạn bất kỳ của quá trình quản lý rủi ro hoặc ở bất kỳ giai đoạn nào trong vòng đời của một hệ thống, bất cứ khi nào cần sự đồng thuận quan điểm của các chuyên gia.

B.3.3 Đầu vào

Tập hợp các phương án theo đó sự đồng thuận là cần thiết.

B.3.4 Quá trình

Một nhóm chuyên gia được đặt câu hỏi bằng cách sử dụng bảng câu hỏi bán cấu trúc. Các chuyên gia không gặp gỡ vì vậy các quan điểm của họ là độc lập.

Quy trình như sau:

- thành lập một nhóm để thực hiện và theo dõi quá trình Delphi;
- lựa chọn một nhóm các chuyên gia (có thể là một hoặc nhiều hội đồng chuyên gia);
- xây dựng một bảng câu hỏi vòng tròn;
- thử nghiệm bảng câu hỏi;
- gửi bảng câu hỏi tới các hội đồng một cách riêng lẻ;
- phân tích và kết hợp thông tin từ vòng trả lời đầu tiên và gửi lại cho các hội đồng;
- các hội đồng trả lời và quá trình được lặp lại đến khi đạt được sự đồng thuận.

B.3.5 Đầu ra

Sự đồng quy theo hướng đồng thuận về vấn đề đặt ra.

B.3.6 Điểm mạnh và hạn chế

Điểm mạnh bao gồm:

- vì các quan điểm được ẩn danh nên có nhiều khả năng bộ lộ các quan điểm không phổ biến;
- tất cả các quan điểm có sức ảnh hưởng như nhau, tránh vấn đề chi phối cá nhân;
- đạt được quyền sở hữu kết quả;
- mọi người không cần tập trung ở một nơi, tại một thời điểm.

Hạn chế bao gồm:

- cần nhiều lao động và tốn nhiều thời gian;
- những người tham gia cần có khả năng thể hiện rõ bản thân bằng văn bản.

B.4 Danh mục kiểm tra

B.4.1 Tổng quan

Danh mục kiểm tra là danh mục các mối nguy, các rủi ro hoặc những sai lỗi trong kiểm soát thường được xây dựng từ kinh nghiệm, cả từ kết quả của đánh giá rủi ro trước đó hoặc từ kết quả của những sai lỗi trong quá khứ.

B.4.2 Sử dụng

Một danh mục kiểm tra có thể được sử dụng để nhận biết các mối nguy và các rủi ro hoặc để đánh giá hiệu lực của việc kiểm soát. Chúng có thể được sử dụng ở bất kỳ giai đoạn nào trong vòng đời của sản phẩm, quá trình hoặc hệ thống. Chúng có thể được sử dụng như một phần của những kỹ thuật đánh giá rủi ro khác nhưng hữu ích nhất khi được áp dụng để kiểm tra mọi thứ đã được đề cập đến sau khi một kỹ thuật sáng tạo hơn nhận biết các vấn đề mới được áp dụng.

B.4.3 Đầu vào

Thông tin và chuyên môn trước đó về vấn đề, để có thể lựa chọn hoặc xây dựng một danh mục kiểm tra liên quan và được xác nhận giá trị tốt nhất.

B.4.4 Quá trình

Quy trình như sau:

- xác định phạm vi hoạt động;
- lựa chọn một danh mục kiểm tra bao trùm thỏa đáng phạm vi. Danh mục kiểm tra cần được lựa chọn cẩn thận cho mục đích này. Ví dụ không thể sử dụng một danh mục kiểm tra việc kiểm soát tiêu chuẩn để nhận biết những mối nguy hoặc rủi ro mới;
- cá nhân hoặc nhóm sử dụng danh mục kiểm tra thực hiện các bước thông qua từng yếu tố của quá trình hoặc hệ thống và xem xét xem các hạng mục của danh mục kiểm tra hiện có hay không.

B.4.5 Đầu ra

Đầu ra phụ thuộc vào giai đoạn của quá trình quản lý rủi ro tại đó chúng được áp dụng. Ví dụ đầu ra có thể là một danh mục các kiểm soát không đầy đủ hoặc một danh mục các rủi ro.

B.4.6 Điểm mạnh và hạn chế

Điểm mạnh của danh mục kiểm tra bao gồm:

- chúng có thể do người không có chuyên môn sử dụng;
- khi được thiết kế tốt, chúng tích hợp lĩnh vực chuyên môn rộng vào một danh mục dễ dàng để sử dụng hệ thống;
- chúng có thể giúp đảm bảo các vấn đề chung không bị bỏ sót.

Hạn chế bao gồm:

- có xu hướng hạn chế trí tưởng tượng trong việc nhận diện các rủi ro;
- đề cập đến "những điều đã biết", chứ không phải "những điều chưa biết" hoặc "điều chưa biết chưa được nhận biết"
- khuyến khích hành vi "tích vào ô";
- có xu hướng dựa trên sự quan sát, do vậy việc bỏ sót các vấn đề không được nhận thấy dễ dàng.

B.5 Phân tích sơ bộ mối nguy (PHA)

B.5.1 Tổng quan

PHA là một phương pháp phân tích quy nạp đơn giản, mục tiêu của phương pháp là nhận biết các mối nguy, các tình huống và sự kiện nguy hại có thể gây hại cho một hoạt động, bộ phận hoặc hệ thống nhất định.

B.5.2 Sử dụng

Phương pháp này thường được thực hiện ngay khi xây dựng một dự án, khi có ít thông tin về các chi tiết thiết kế hoặc các quy trình vận hành và thường có thể là một yếu tố dự báo để nghiên cứu thêm hoặc để cung cấp thông tin đối với quy định thiết kế một hệ thống. Cũng có thể hữu ích khi phân tích các hệ thống hiện có để thiết lập thứ tự ưu tiên những mối nguy và rủi ro cho việc phân tích thêm hoặc trong các trường hợp ngăn cản việc sử dụng một kỹ thuật rộng hơn.

B.5.3 Đầu vào

Đầu vào bao gồm:

- thông tin về hệ thống được đánh giá;
- chi tiết về thiết kế hệ thống sẵn có và phù hợp.

B.5.4 Quá trình

Một danh mục các mối nguy, các tình huống nguy hại và các rủi ro được hình thành bằng cách xem xét các đặc trưng như:

- các vật liệu được sử dụng hoặc được sản xuất và hoạt tính của chúng;
- thiết bị làm việc;
- môi trường hoạt động;
- bố trí;
- điểm tương giao giữa các thành phần của hệ thống, v.v...

Phân tích định tính về hệ quả của một sự kiện không mong muốn và xác suất của chúng có thể được thực hiện để nhận diện rủi ro của việc đánh giá thêm.

PHA cần được cập nhật trong các giai đoạn thiết kế, xây dựng và thử nghiệm để phát hiện bất kỳ mối nguy mới nào và thực hiện điều chỉnh khi cần. Các kết quả thu được có thể được thể hiện theo nhiều cách khác nhau như dạng bảng và cây.

B.5.5 Đầu ra

Đầu ra bao gồm:

- danh mục các mối nguy và rủi ro;
- khuyến nghị về các hình thức chấp nhận, những kiểm soát được khuyến nghị, quy định hoặc các yêu cầu thiết kế cho việc đánh giá chi tiết hơn.

B.5.6 Điểm mạnh và hạn chế

Điểm mạnh bao gồm:

- phương pháp có thể được sử dụng khi thông tin hạn chế;
- cho phép xem xét sớm các rủi ro trong vòng đời hệ thống.

Hạn chế bao gồm:

- PHA chỉ cung cấp thông tin sơ bộ; nó chưa toàn diện cũng như không cung cấp thông tin chi tiết về những rủi ro và cách thức có thể ngăn chặn chúng tốt nhất.

B.6 HAZOP

B.6.1 Tổng quan

HAZOP là cụm từ viết tắt tiếng Anh của nghiên cứu mối nguy, khả năng vận hành, là việc kiểm tra có cấu trúc, hệ thống về một sản phẩm, quá trình, quy trình hoặc hệ thống được hoạch định hoặc hiện có. Đây là một kỹ thuật để nhận diện những rủi ro cho con người, thiết bị, môi trường và/hoặc các mục tiêu

của tổ chức. Khi có thể, nhóm nghiên cứu cũng được mong đợi đưa ra giải pháp xử lý rủi ro.

Quá trình HAZOP là một kỹ thuật định tính dựa trên việc sử dụng các từ hướng dẫn đặt câu hỏi về cách thức mục đích thiết kế hoặc các điều kiện hoạt động có thể không đạt được ở mỗi giai đoạn thiết kế, quá trình, quy trình hoặc hệ thống. Phương pháp này thường do một nhóm đa ngành thực hiện trong một loạt các cuộc họp.

HAZOP cũng tương tự như FMEA trong đó nhận biết các phương thức sai lỗi của một quá trình, hệ thống hoặc quy trình, các nguyên nhân và hệ quả của chúng. Nó khác với FMEA ở chỗ nhóm xem xét các kết quả ngoài dự kiến và những sai lệch so với kết quả dự kiến và các điều kiện, công việc ngược trở lại tới các nguyên nhân và các phương thức sai lỗi có thể, trong khi FMEA bắt đầu bằng việc nhận biết các phương thức sai lỗi.

B.6.2 Sử dụng

Ban đầu kỹ thuật HAZOP được xây dựng để phân tích các hệ thống quá trình hóa học, nhưng đã được mở rộng cho các loại hệ thống và hoạt động phức tạp khác. Những hệ thống và hoạt động này bao gồm các hệ thống quy trình điện tử và cơ khí, các hệ thống phần mềm và thậm chí đối với sự thay đổi của tổ chức cũng như đối với việc xem xét và thiết kế hợp đồng pháp lý.

Quá trình HAZOP có thể xử lý tất cả các hình thức sai lệch so với mục đích thiết kế do những thiếu sót trong thiết kế, (các) yếu tố, các quy trình được hoạch định và những hành động của con người.

Nó được sử dụng rộng rãi cho việc xem xét thiết kế phần mềm. Khi được áp dụng cho các hệ thống máy tính và kiểm soát công cụ an toàn quan trọng, nó có thể được biết đến là CHAZOP (kiểm soát phân tích mối nguy và khả năng vận hành hoặc phân tích mối nguy và khả năng vận hành của máy tính).

Nghiên cứu HAZOP thường được thực hiện ở giai đoạn thiết kế chi tiết, khi sẵn có một biểu đồ đầy đủ về quá trình dự kiến, nhưng vẫn có thể xảy ra những thay đổi thiết kế. Tuy nhiên nó có thể được thực hiện theo cách tiếp cận theo giai đoạn với những hướng dẫn khác nhau cho từng giai đoạn như xây dựng thiết kế chi tiết. Nghiên cứu HAZOP cũng có thể được thực hiện trong vận hành nhưng những thay đổi cần thiết có thể là tốn kém ở giai đoạn đó.

B.6.3 Đầu vào

Đầu vào thiết yếu cho một nghiên cứu HAZOP bao gồm thông tin hiện tại về hệ thống, quá trình hoặc quy trình được xem xét và các quy định về mục đích và tính năng của thiết kế. Đầu vào có thể bao gồm: các bản vẽ, phiếu quy định, phiếu lưu đồ, kiểm soát quá trình và các biểu đồ logic, các bản vẽ về cách bố trí, các quy trình vận hành và bảo trì và các quy trình ứng phó tình trạng khẩn cấp. Đối với phần không phải là phần cứng liên quan đến đầu vào của HAZOP có thể là bất kỳ tài liệu nào mô tả các chức năng và yếu tố của hệ thống hoặc quy trình được nghiên cứu. Ví dụ, đầu vào có thể là các sơ đồ tổ chức và mô tả vai trò, dự thảo hợp đồng hoặc thậm chí dự thảo quy trình.

B.6.4 Quá trình

HAZOP thực hiện "thiết kế" và quy định của quá trình, quy trình hoặc hệ thống được nghiên cứu và xem xét từng phần của nó để tìm ra những sai lệch so với việc thực hiện dự kiến có thể xảy ra, các nguyên nhân tiềm ẩn là gì và hệ quả nào có thể xảy ra từ những sai lệch đó. Điều này đạt được bằng cách kiểm tra một cách hệ thống cách thức mỗi phần của hệ thống, quá trình hoặc quy trình đáp ứng những thay đổi theo các thông số chính bằng cách sử dụng các từ hướng dẫn phù hợp. Các từ hướng dẫn có thể được điều chỉnh theo một hệ thống, quá trình hoặc quy trình cụ thể hoặc các từ chung có thể được sử dụng bao gồm tất cả các loại sai lệch. Bảng B.1 đưa ra các ví dụ về các từ hướng dẫn thường được sử dụng phổ biến cho các hệ thống kỹ thuật. Các từ hướng dẫn tương tự như 'quá sớm', 'quá muộn', 'quá nhiều', 'quá ít', 'quá dài', 'quá ngắn', 'sai hướng', 'sai đối tượng', 'hành động sai' có thể được sử dụng để nhận biết các phương thức sai lỗi của con người.

Các bước thông thường trong một nghiên cứu HAZOP bao gồm:

- chỉ định người có trách nhiệm và quyền hạn cần thiết để tiến hành nghiên cứu HAZOP và để đảm bảo rằng mọi hành động nảy sinh từ nghiên cứu được hoàn thành;
- xác định các mục tiêu và phạm vi nghiên cứu;
- thiết lập một tập hợp các từ khóa hoặc các từ hướng dẫn cho nghiên cứu;
- xác định nhóm nghiên cứu HAZOP; nhóm này thường là đa ngành và cần bao gồm nhân sự thiết kế và vận hành có chuyên môn kỹ thuật thích hợp để đánh giá tác động của những sai lệch so với thiết kế dự kiến hoặc hiện tại. Khuyến nghị rằng nhóm bao gồm những người không liên quan trực tiếp tới thiết kế hoặc hệ thống, quá trình hoặc quy trình được xem xét;
- thu thập tài liệu cần thiết.

Trong một cuộc hội thảo được hỗ trợ với nhóm nghiên cứu:

- phân chia hệ thống, quá trình hoặc quy trình thành các thành phần nhỏ hơn hoặc các hệ thống con hay quá trình con hoặc các thành phần con để đưa ra sự xem xét rõ ràng;
- thống nhất về mục đích thiết kế đối với mỗi hệ thống con, quá trình con hoặc thành phần con và sau đó cho từng hạng mục trong hệ thống con hoặc thành phần áp dụng những hướng dẫn nối tiếp nhau để thừa nhận những sai lệch có thể sẽ có các kết quả không mong muốn;
- khi một kết quả không mong muốn được nhận biết, thống nhất về nguyên nhân và hệ quả trong mỗi trường hợp và gợi ý cách thức chúng có thể được xử lý để ngăn chặn việc xảy ra hoặc giảm nhẹ các hệ quả nếu xảy ra;
- lập thành văn bản cuộc thảo luận và thống nhất các hành động cụ thể để xử lý rủi ro được nhận biết.

Bảng B.1 – Ví dụ về các từ hướng dẫn có thể trong HAZOP

Thuật ngữ	Định nghĩa
Không có hoặc không	Không đạt được phần nào của kết quả dự kiến hoặc thiếu điều kiện dự kiến
Nhiều hơn (cao hơn)	Đầu ra hoặc điều kiện hoạt động tăng lên về lượng
Ít hơn (thấp hơn)	Giảm về lượng
Như nhau	Tăng về lượng (ví dụ nguyên liệu bổ sung)
Một phần	Giảm về lượng (ví dụ chỉ một hoặc hai thành phần trong một hỗn hợp)
Nghịch đảo /đối lập	Sự đối lập (ví dụ chảy ngược lại)
Khác với	Không đạt được phần nào của ý định, một điều gì đó xảy ra hoàn toàn khác
	(ví dụ dòng chảy hoặc nguyên liệu sai)
Tính tương thích	Nguyên liệu; môi trường
Các từ hướng dẫn được áp dụng cho các thông số như là	
	Tính chất vật lý của vật liệu hoặc quá trình
	Các điều kiện vật lý như là nhiệt độ, tốc độ
	Một mục đích quy định về một yếu tố của hệ thống hoặc thiết kế (ví dụ truyền thông tin)
	Các khía cạnh về vận hành

B.6.5 Đầu ra

Biên bản của (các) cuộc họp HAZOP với những hạng mục cho mỗi điểm xem xét được lưu hồ sơ. Điều này cần bao gồm: từ hướng dẫn được sử dụng, (các) sai lệch, các nguyên nhân có thể, các hành động để giải quyết các vấn đề được nhận biết và người chịu trách nhiệm về hành động.

Đối với mọi sai lệch không thể được điều chỉnh, thì rủi ro đối với sai lệch đó cần được đánh giá.

B.6.6 Điểm mạnh và hạn chế

Phân tích HAZOP có những ưu điểm sau:

- đưa ra biện pháp kiểm tra một cách hệ thống và kỹ lưỡng quá trình hoặc quy trình;
- lôi kéo sự tham gia của một nhóm đa ngành bao gồm những người có kinh nghiệm hoạt động thực tế và những người có thể phải thực hiện các hành động xử lý;
- tạo ra các giải pháp và các hành động xử lý rủi ro;
- thích hợp với một phạm vi rộng các hệ thống, các quá trình và quy trình;
- cho phép xem xét rõ ràng các nguyên nhân và hệ quả do sai lỗi của con người;
- tạo ra một hồ sơ bằng văn bản về các quá trình có thể được sử dụng để chứng minh sự tích cực.

Hạn chế bao gồm:

- phân tích chi tiết có thể tốn nhiều thời gian và do đó sẽ tốn kém;
- phân tích chi tiết đòi hỏi một mức độ văn bản hóa cao hoặc quy định về hệ thống/quá trình và quy

trình;

- nó có thể chú trọng vào việc tìm kiếm các giải pháp chi tiết thay vì nghi ngờ các giả định cơ bản (tuy nhiên, có thể giảm nhẹ điều này bằng một cách tiếp cận theo giai đoạn);
- cuộc thảo luận có thể tập trung vào các vấn đề thiết kế chi tiết chứ không phải các vấn đề rộng hơn hoặc vấn đề bên ngoài;
- nó bị ràng buộc bởi (dự thảo) thiết kế và mục đích thiết kế và phạm vi và các mục tiêu đưa ra cho nhóm;
- quá trình dựa nhiều vào chuyên môn của các nhà thiết kế, họ có thể thấy khó khăn để hoàn toàn khách quan trong việc tìm kiếm các vấn đề trong các thiết kế của mình.

B.6.7 Tài liệu viện dẫn

IEC 61882, N*ghiên cứu mối nguy và khả năng vận hành (nghiên cứu HAZOP) – Hướng dẫn áp dụng.*

B.7 Phân tích mối nguy và điểm kiểm soát trọng yếu (HACCP)

B.7.1 Tổng quan

Phân tích mối nguy và điểm kiểm soát trọng yếu (HACCP) đưa ra một cấu trúc cho việc nhận biết các mối nguy và đưa vào kiểm soát ở tất cả các phần liên quan của một quá trình để bảo vệ khỏi các mối nguy và duy trì sự tin cậy vào chất lượng và an toàn của sản phẩm. HACCP nhằm đảm bảo rằng các rủi ro được tối thiểu hóa bằng các kiểm soát toàn bộ quá trình hơn là thông qua kiểm tra sản phẩm cuối cùng.

B.7.2 Sử dụng

HACCP được xây dựng để đảm bảo chất lượng thực phẩm cho chương trình không gian của NASA. Hiện nay nó do các tổ chức hoạt động ở bất kỳ khâu nào trong chuỗi thực phẩm sử dụng để kiểm soát các rủi ro từ các chất gây ô nhiễm vật lý, hóa học hoặc sinh học cho thực phẩm. Nó cũng được mở rộng để sử dụng trong việc sản xuất dược phẩm và thiết bị y tế. Nguyên tắc của việc nhận biết những điều có thể ảnh hưởng đến chất lượng sản phẩm và xác định các điểm trong một quá trình tại đó các thông số trọng yếu có thể được theo dõi và các mối nguy được kiểm soát, có thể được khái quát hóa cho các hệ thống kỹ thuật khác.

B.7.3 Đầu vào

HACCP bắt đầu từ một sơ đồ dòng chảy cơ bản hoặc sơ đồ và quá trình thông tin về những mối nguy có thể ảnh hưởng đến chất lượng, an toàn hoặc độ tin cậy của sản phẩm hoặc đầu ra của quá trình. Thông tin về những mối nguy và rủi ro của chúng và cách thức chúng có thể được kiểm soát là một đầu vào cho HACCP.

B.7.4 Quá trình

HACCP bao gồm bảy nguyên tắc như sau:

- nhận biết các mối nguy và các biện pháp ngăn ngừa liên quan đến những mối nguy này;

- xác định các điểm trong quá trình tại đó các mối nguy có thể được kiểm soát hoặc loại bỏ (điểm kiểm soát trọng yếu hoặc các CCP);
- thiết lập các giới hạn tới hạn cần thiết để kiểm soát các mối nguy, nghĩa là mỗi CCP cần vận hành trong phạm vi các thông số cụ thể để đảm bảo kiểm soát mối nguy;
- theo dõi các giới hạn tới hạn đối với mỗi CCP theo khoảng thời gian xác định;
- thiết lập các hành động khắc phục nếu quá trình nằm ngoài các giới hạn được thiết lập;
- thiết lập các quy trình kiểm tra xác nhận;
- thực hiện lưu giữ hồ sơ và các quy trình bằng văn bản đối với mỗi giai đoạn.

B.7.5 Đầu ra

Các hồ sơ được lập thành văn bản bao gồm một bảng phân tích mối nguy và một kế hoạch HACCP.

Bảng phân tích mối nguy liệt kê những nội dung sau cho từng bước của quá trình:

- những mối nguy có thể được giới thiệu, được kiểm soát hoặc làm trầm trọng hơn ở bước này;
- các mối nguy có thể hiện một rủi ro đáng kể hay không (dựa trên việc xem xét hệ quả và xác suất từ sự kết hợp giữa kinh nghiệm, dữ liệu và các tài liệu kỹ thuật);
- lý giải cho mức độ đáng kể;
- các biện pháp ngăn ngừa có thể đối với mỗi mối nguy;
- có thể áp dụng các biện pháp theo dõi hoặc kiểm soát ở giai đoạn này hay không (nghĩa là đây có phải là một CCP không?).

Kế hoạch HACCP mô tả các quy trình được tuân thủ để đảm bảo kiểm soát một thiết kế, sản phẩm, quá trình hoặc quy trình cụ thể. Kế hoạch này bao gồm một danh mục tất cả các CCP và đối với mỗi CCP:

- giới hạn tới hạn đối với các biện pháp phòng ngừa;
- các hoạt động theo dõi và kiểm soát liên tục (bao gồm thực hiện theo dõi những gì, như thế nào, khi nào và ai thực hiện);
- các hành động khắc phục cần thiết nếu phát hiện những sai lệch so với những giới hạn tới hạn;
- các hoạt động kiểm tra xác nhận và lưu giữ hồ sơ.

B.7.6 Điểm mạnh và giới hạn

Điểm mạnh bao gồm:

- một quá trình được cấu trúc đưa ra bằng chứng dạng văn bản đối với việc kiểm soát chất lượng cũng như việc nhận biết và làm giảm rủi ro;
- tập trung vào khả năng thực tiễn, cách thức và vị trí trong một quá trình, các mối nguy có thể được ngăn ngừa và những rủi ro được kiểm soát;

- kiểm soát rủi ro tốt hơn trong suốt quá trình thay vì dựa vào kiểm tra sản phẩm cuối cùng;
- khả năng nhận biết các mối nguy được đưa vào thông qua hành động của con người và cách thức những rủi ro này có thể được kiểm soát tại điểm đưa vào hoặc sau đó.

Hạn chế bao gồm:

- HACCP yêu cầu nhận biết các mối nguy, xác định những rủi ro mà chúng đại diện, ý nghĩa của chúng được hiểu là các đầu vào đối với quá trình. Các kiểm soát thích hợp cũng cần được xác định. Những điều này được yêu cầu để quy định các điểm kiểm soát trọng yếu và các thông số kiểm soát trong HACCP và có thể cần được kết hợp với các công cụ khác để đạt được điều này;
- việc thực hiện hành động khi các thông số kiểm soát vượt quá những giới hạn xác định có thể bỏ sót những thay đổi từng bước trong các thông số kiểm soát có ý nghĩa về mặt thống kê và do đó cần được hành động.

B.7.7 Tài liệu viện dẫn

TCVN ISO 22000, *Hệ thống quản lý an toàn thực phẩm – Yêu cầu đối với tổ chức trong chuỗi thực phẩm.*

B.8 Đánh giá tính độc hại

B.8.1 Tổng quát

Ở đây, đánh giá rủi ro về môi trường được sử dụng để bao trùm quá trình được tuân theo khi đánh giá rủi ro với thực vật, động vật và con người là kết quả của việc hứng chịu một loạt các mối nguy về môi trường. Quản lý rủi ro đề cập đến các bước ra quyết định bao gồm định mức rủi ro và xử lý rủi ro.

Phương pháp này đòi hỏi việc phân tích mối nguy hoặc nguồn gây hại và cách thức ảnh hưởng đến tổng thể mục tiêu và cách thức theo đó mối nguy có thể đạt tới tổng thể mục tiêu dễ bị ảnh hưởng. Thông tin này sau đó được kết hợp để đưa ra một ước lượng về mức độ và tính chất của tác hại có thể xảy ra.

B.8.2 Sử dụng

Quá trình này được sử dụng để đánh giá những rủi ro đối với thực vật, động vật và con người do việc hứng chịu những mối nguy như hóa chất, vi sinh vật hoặc các loài khác.

Các khía cạnh của phương pháp luận, như phân tích cách thức theo đó khai thác các lộ trình khác nhau trong đó mục tiêu có thể hứng chịu một nguồn rủi ro, có thể được thích ứng và sử dụng trên một phạm vi rất rộng các lĩnh vực rủi ro khác nhau ngoài sức khỏe con người và môi trường và hữu ích trong việc nhận biết biện pháp xử lý để giảm bớt rủi ro.

B.8.3 Đầu vào

Phương pháp này đòi hỏi dữ liệu tốt về bản chất và thuộc tính của các mối nguy, điểm yếu của tổng thể mục tiêu (hoặc các tổng thể) và cách thức trong đó hai yếu tố tác động lẫn nhau. Dữ liệu này

thường được dựa trên nghiên cứu có thể trên cơ sở phòng thí nghiệm hoặc dịch y tế.

B.8.4 Quá trình

Quy trình như sau:

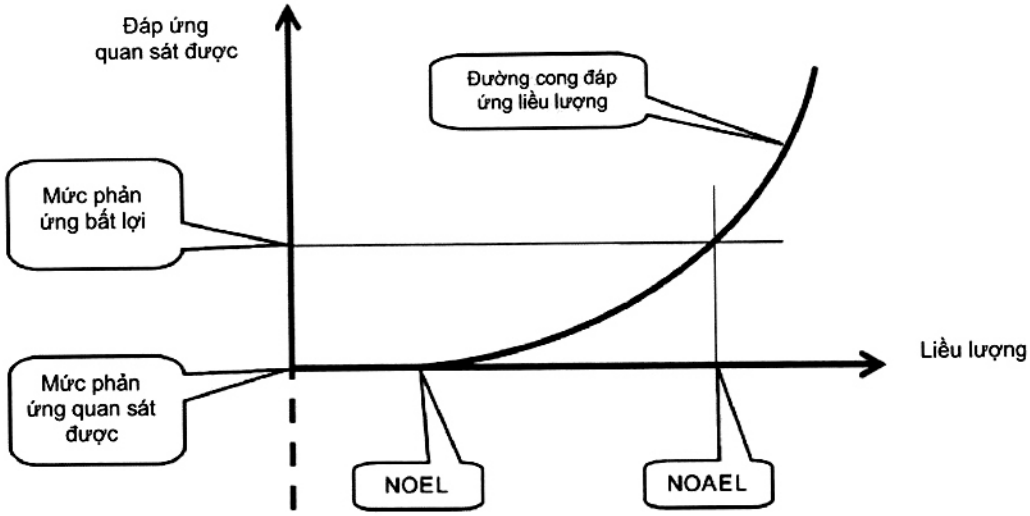
a) Hình thành vấn đề – điều này bao gồm việc thiết lập phạm vi của việc đánh giá bằng cách xác định phạm vi của tổng thể mục tiêu và loại mối nguy được quan tâm;

b) Nhận biết mối nguy – điều này đòi hỏi việc nhận biết tất cả các nguồn tác hại có thể đối với tổng thể mục tiêu từ những mối nguy trong phạm vi nghiên cứu. Việc nhận biết mối nguy thường dựa vào kiến thức chuyên môn và việc xem xét tài liệu khoa học;

c) Phân tích mối nguy – điều này đòi hỏi việc hiểu rõ bản chất của mối nguy và cách thức nó tương tác với mục tiêu. Ví dụ, khi xem xét việc phơi nhiễm của con người với các tác động hóa học, mối nguy có thể bao gồm độc hại tức thời và lâu dài, khả năng hủy hoại ADN hoặc khả năng gây ra ung thư hay các dị tật bẩm sinh. Đối với mỗi tác động nguy hại, mức độ tác động (đáp ứng) được so sánh với số lượng mối nguy tại đó mục tiêu phải hứng chịu (liều lượng) và khi có thể, cơ chế theo đó tác động được sinh ra được xác định. Các mức tại đó có tác động không thấy được (NOEL) và tác động có hại không thấy được (NOAEL) được ghi lại. Đôi khi các mức được sử dụng làm tiêu chí cho việc chấp nhận rủi ro.

   Đối với việc hứng chịu hóa chất, các kết quả thử nghiệm được sử dụng để suy ra đường cong đáp ứng liều lượng như được biểu diễn dưới dạng biểu đồ trong Hình B.1. Kết quả thường được bắt nguồn từ các phép thử trên động vật hoặc từ các hệ thống thực nghiệm như mô hoặc tế bào nuôi cấy.

   Tác động của các mối nguy khác như là vi sinh vật hoặc các loài đã nêu có thể được xác định từ dữ liệu của lĩnh vực và nghiên cứu dịch tễ học. Bản chất của sự tương tác giữa dịch bệnh vi khuẩn gây bệnh với mục tiêu được xác định và xác suất một mức tác hại cụ thể từ việc hứng chịu cụ thể mối nguy được ước lượng.



Hình B.1 – Đường cong đáp ứng liều lượng

d) Phân tích phơi nhiễm – bước này kiểm tra cách thức một chất độc hại hoặc tồn dư của nó có thể đạt tới tổng thể mục tiêu dễ bị ảnh hưởng và với số lượng bao nhiêu. Nó thường đòi hỏi phân tích theo lộ trình trong đó xem xét các con đường khác nhau của mối nguy, các rào cản có thể ngăn cản nó đạt tới mục tiêu và các yếu tố có thể ảnh hưởng đến mức phơi nhiễm. Ví dụ, khi xem xét rủi ro từ việc phun hóa chất, việc phân tích phơi nhiễm sẽ xem xét có bao nhiêu hóa chất được phun, theo cách nào và với điều kiện gì, có các phơi nhiễm trực tiếp của con người hoặc động vật hay không, có thể để lại bao nhiêu dư lượng trên đời sống thực vật, sự hủy diệt môi trường của thuốc trừ sâu với đất, nó có thể tích lũy trong động vật hay không hoặc nó có xâm nhập vào nước ngầm không. Trong an ninh sinh học, phân tích theo lộ trình có thể xem xét các thức bất kỳ sinh vật gây bệnh nào xâm nhập vào quốc gia có thể xâm nhập vào môi trường, bị đưa vào và lây lan.

e) Mô tả đặc trưng rủi ro – trong bước này, thông tin từ phân tích mối nguy và phân tích phơi nhiễm được tập hợp lại để ước lượng xác suất của hệ quả cụ thể khi kết hợp những tác động từ tất cả các lộ trình. Nếu có một số lượng lớn các mối nguy hoặc các lộ trình, sự sàng lọc ban đầu có thể được thực hiện và phân tích mối nguy và phơi nhiễm chi tiết và mô tả đặc trưng rủi ro được thực hiện trên tình huống rủi ro cao hơn.

B.8.5 Đầu ra

Đầu ra thường là một chỉ dẫn về mức rủi ro từ việc phơi nhiễm của mục tiêu cụ thể với một mối nguy cụ thể trong bối cảnh có liên quan. Rủi ro có thể được thể hiện định lượng, bán định lượng hoặc định tính. Ví dụ, rủi ro bị ung thư thường được thể hiện định lượng như xác suất, rằng một người sẽ phát triển bệnh ung thư trong một khoảng thời gian quy định với sự phơi nhiễm nhất định đối với một chất ô

nhiễm. Phân tích bán định lượng có thể được sử dụng để có được một chỉ số rủi ro đối với một chất ô nhiễm hoặc sinh vật gây bệnh cụ thể và đầu ra định tính có thể là một mức rủi ro (ví dụ cao, trung bình, thấp) hoặc một mô tả với dữ liệu thực tế về tác động có thể có.

B.8.6 Điểm mạnh và hạn chế

Điểm mạnh của việc phân tích này là đưa ra một sự hiểu biết rất chi tiết về bản chất của vấn đề và các yếu tố làm tăng rủi ro.

Nói chung, phân tích theo lộ trình là một công cụ hữu ích cho tất cả các lĩnh vực rủi ro và cho phép nhận biết cách thức và vị trí có thể cải tiến việc kiểm soát hoặc đưa vào các kiểm soát mới.

Tuy nhiên nó cần các dữ liệu tốt và thường không sẵn có hoặc có độ không đảm bảo cao kèm theo. Ví dụ, đường cong đáp ứng liều lượng bắt nguồn từ phơi nhiễm động vật với mối nguy ở mức độ cao cần được ngoại suy để ước tính những tác động về mức độ chất gây ô nhiễm rất thấp tới con người và có nhiều mô hình trong đó điều này có thể đạt được. Khi mục tiêu là môi trường chứ không phải là con người và mối nguy không phải là hóa chất, thì dữ liệu liên quan trực tiếp tới các điều kiện cụ thể của nghiên cứu có thể hạn chế.

B.9 Kỹ thuật cấu trúc "Điều gì-nếu" (SWIFT)

B.9.1 Tổng quan

Ban đầu, SWIFT được xây dựng như một giải pháp thay thế đơn giản hơn HAZOP. Nó là một nghiên cứu có hệ thống theo nhóm, sử dụng một tập hợp các từ hoặc câu "gợi ý" được người trợ giúp sử dụng trong một hội thảo để khuyến khích những người tham gia nhận biết các rủi ro. Người hỗ trợ và nhóm sử dụng câu chuẩn loại "Điều gì - nếu" kết hợp với các gợi ý để điều tra về cách thức một hệ thống, đối tượng thực vật, tổ chức hoặc quy trình sẽ bị tác động bởi sự sai lệch khỏi việc vận hành và hành vi thông thường. SWIFT thường được áp dụng ở một mức độ hệ thống hơn với một mức độ chi tiết thấp hơn HAZOP.

B.9.2 Sử dụng

Nếu như ban đầu SWIFT được thiết kế để nghiên cứu mối nguy cho nhà máy hóa chất và hóa dầu thì hiện nay kỹ thuật này được áp dụng rộng rãi cho các hệ thống, đối tượng thực vật, các quy trình, tổ chức nói chung. Đặc biệt nó được sử dụng để kiểm tra hệ quả của những thay đổi và do đó các rủi ro bị thay đổi hoặc được tạo ra.

B.9.3 Đầu vào

Hệ thống, quy trình, đối tượng thực vật và/hoặc thay đổi phải được xác định cẩn thận trước khi việc nghiên cứu có thể bắt đầu. Cả bối cảnh nội bộ và bên ngoài đều được người hỗ trợ thiết lập thông qua phỏng vấn và thông qua việc nghiên cứu các tài liệu, kế hoạch và bản vẽ. Thông thường, đối tượng, tình huống hoặc hệ thống cho nghiên cứu được chia ra thành các nút hoặc các yếu tố chính để tạo thuận lợi cho phân tích quá trình nhưng điều này hiếm khi xảy ra ở mức độ xác định cần thiết cho

HAZOP.

Một đầu vào quan trọng khác là chuyên môn và kinh nghiệm thể hiện trong nhóm nghiên cứu cần được lựa chọn cẩn thận. Tất cả các bên liên quan cần được đại diện khi có thể bởi với những người có kinh nghiệm về các đối tượng, hệ thống, sự thay đổi hoặc tình huống tương tự.

B.9.4 Quá trình

Quá trình chung như sau:

a) Trước khi bắt đầu nghiên cứu, người hỗ trợ chuẩn bị danh mục các từ hoặc câu gợi ý thích hợp có thể dựa trên một bộ tiêu chuẩn hoặc được tạo ra để có thể việc xem xét các mối nguy hoặc các rủi ro toàn diện.

b) Tại hội thảo, bối cảnh nội bộ và bên ngoài của đối tượng, hệ thống, sự thay đổi hoặc tình huống và phạm vi nghiên cứu được thảo luận và thống nhất.

c) Người hỗ trợ yêu cầu người tham gia nêu và thảo luận:

- những rủi ro và mối nguy được biết đến;
- kinh nghiệm và các sự cố trước đó;
- kiểm soát và các biện pháp bảo vệ hiện có và được biết đến;
- các yêu cầu và ràng buộc chế định.

d) Thảo luận được tạo điều kiện bằng cách tạo ra câu hỏi sử dụng mẫu câu 'điều gì-nếu' và một từ hoặc đối tượng gợi ý. Các câu 'điều gì-nếu' được sử dụng là "điều gì nếu....", "điều gì sẽ xảy ra nếu...", "ai hoặc điều gì đó có thể....", "ai hay điều gì đã từng....". Mục đích là để khuyến khích nhóm nghiên cứu tìm hiểu tình huống tiềm ẩn, các nguyên nhân, hệ quả và tác động của chúng.

e) Các rủi ro được tóm tắt và nhóm xem xét đưa ra các kiểm soát.

f) Mô tả rủi ro, các nguyên nhân, hệ quả của rủi ro và kiểm soát dự kiến được xác nhận với nhóm và được lưu hồ sơ.

g) Nhóm xem xét xem các kiểm soát có đầy đủ và hiệu lực hay không và thống nhất một tuyên bố về hiệu lực kiểm soát rủi ro. Nếu điều này ít thỏa mãn hơn, nhóm tiếp tục xem xét các nhiệm vụ xử lý rủi ro và xác định các kiểm soát tiềm ẩn.

h) Trong cuộc thảo luận này các câu hỏi 'điều gì – nếu' tiếp tục được đưa ra để nhận biết thêm các rủi ro.

i) Người hỗ trợ sử dụng danh mục gợi ý để theo dõi cuộc thảo luận và để gợi ý các vấn đề và tình huống bổ sung cho nhóm để thảo luận.

j) Thường sử dụng một phương pháp đánh giá rủi ro định tính hoặc bán định lượng để sắp xếp các hành động được tạo theo thứ tự ưu tiên. Đánh giá rủi ro này thường được thực hiện bằng cách tính đến các kiểm soát hiện có và hiệu lực của chúng.

B.9.5 Đầu ra

Đầu ra bao gồm nhật ký rủi ro với các hành động hoặc nhiệm vụ được xếp hạng theo rủi ro. Những nhiệm vụ này sau đó có thể trở thành cơ sở cho kế hoạch xử lý.

B.9.6 Điểm mạnh và hạn chế

Điểm mạnh của SWIFT:

- áp dụng rộng rãi cho tất cả các hình thức của nhà máy, hệ thống, tình huống hoặc các trường hợp, tổ chức hoặc hoạt động vật lý;
- cần chuẩn bị tối thiểu theo từng nhóm;
- tương đối nhanh chóng, các mối nguy và rủi ro chính nhanh chóng trở nên rõ ràng trong cuộc hội thảo;
- nghiên cứu mang tính "định hướng hệ thống" và cho phép những người tham gia xem xét đáp ứng của hệ thống với những sai lệch thay vì kiểm tra những hệ quả của sai lỗi thành phần;
- có thể được sử dụng để nhận biết các cơ hội cải tiến quá trình và hệ thống và nhìn chung có thể được sử dụng để nhận biết các hành động dẫn đến và nâng cao xác suất thành công của chúng;
- việc tham gia vào hội thảo của những người chịu trách nhiệm với việc kiểm soát hiện có và cho các hành động xử lý rủi ro tiếp theo, sẽ nâng cao trách nhiệm của họ;
- nó tạo ra danh mục rủi ro và kế hoạch xử lý rủi ro với nỗ lực ít hơn;
- do thường sử dụng hình thức xếp hạng rủi ro định tính hoặc bán định lượng để đánh giá rủi ro và để tối ưu hóa sự tập trung vào các hành động kết quả, nên SWIFT có thể được sử dụng để nhận biết các rủi ro và mối nguy có thể theo đuổi vào một nghiên cứu định lượng.

Hạn chế của SWIFT:

- cần một người hỗ trợ có kinh nghiệm và khả năng thì mới có hiệu quả;
- cần chuẩn bị kỹ lưỡng để không lãng phí thời gian hội thảo nhóm;
- nếu nhóm hội thảo không có một nền tảng kinh nghiệm đủ rộng hoặc nếu hệ thống gợi ý không toàn diện, một số rủi ro và mối nguy có thể không được nhận diện;
- ứng dụng kỹ thuật này ở mức độ cao có thể không bộc lộ các nguyên nhân phức tạp, chi tiết hoặc tương quan.

B.10 Phân tích kịch bản

B.10.1 Tổng quan

Phân tích kịch bản là tên được đưa ra đối với việc xây dựng mô hình mô tả về cách thức tương lai có thể xảy ra. Nó có thể được sử dụng để nhận biết rủi ro bằng cách xem xét sự phát triển tương lai có

thể có và khám phá những ẩn ý của chúng. Tập hợp các kịch bản phản ánh (ví dụ) 'trường hợp tốt nhất', 'trường hợp xấu nhất' và 'trường hợp được mong đợi' có thể được sử dụng để phân tích hệ quả tiềm ẩn và xác suất của chúng đối với mỗi kịch bản dưới dạng phân tích độ nhạy khi phân tích rủi ro.

Khả năng phân tích kịch bản được minh họa bằng cách xem xét sự thay đổi lớn về công nghệ, sở thích của người tiêu dùng, thái độ xã hội, v.v....trong vòng 50 năm qua. Phân tích kịch bản không thể dự đoán xác suất của những thay đổi này nhưng có thể xem xét hệ quả và giúp các tổ chức phát triển điểm mạnh và khả năng thích ứng cần thiết để thích ứng với những thay đổi có thể dự báo.

B.10.2 Sử dụng

Phân tích kịch bản có thể được sử dụng để hỗ trợ trong việc ra quyết định chính sách và hoạch định chiến lược tương lai cũng như xem xét các hoạt động hiện tại. Nó có thể là một phần trong ba thành tố của đánh giá rủi ro. Đối với việc nhận diện và phân tích, tập hợp các kịch bản phản ánh (ví dụ) trường hợp tốt nhất, trường hợp xấu nhất và trường hợp 'được mong đợi' có thể được sử dụng để nhận biết những điều có thể xảy ra theo những kịch bản cụ thể và phân tích hệ quả tiềm ẩn và xác suất của chúng đối với mỗi kịch bản.

Phân tích kịch bản có thể được sử dụng để dự đoán cách thức cả những đe dọa và cơ hội có thể phát triển và có thể được sử dụng cho tất cả các loại rủi ro với khung thời gian ngắn hạn và dài hạn. Với khung thời gian ngắn hạn và dữ liệu tốt, các kịch bản có thể xảy ra có thể được ngoại suy từ hiện tại. Đối với khung thời gian dài hơn hoặc với dữ liệu kém, Phân tích kịch bản sẽ mang tính tưởng tượng hơn và có thể được đề cập đến như là phân tích tương lai.

Phân tích kịch bản có thể là hữu ích khi có sự khác nhau lớn về phân bố giữa các kết quả tích cực và kết quả tiêu cực theo không gian, thời gian và các nhóm trong cộng đồng hoặc một tổ chức.

B.10.3 Đầu ra

Điều tiên quyết đối với phân tích kịch bản là một nhóm người, giữa họ có một sự hiểu biết về bản chất của sự thay đổi liên quan (ví dụ sự tiến bộ có thể có về công nghệ) và tưởng tượng để nghĩ về tương lai mà không nhất thiết phải ngoại suy từ quá khứ. Tiếp cận tài liệu khoa học và dữ liệu về những thay đổi đã xảy ra cũng rất hữu ích.

B.10.4 Quá trình

Cấu trúc trong phân tích kịch bản có thể là chính thức hoặc không chính thức.

Sau khi thành lập một nhóm và các kênh trao đổi thông tin phù hợp và xác định bối cảnh của vấn đề và các vấn đề được xem xét, bước tiếp theo là nhận biết bản chất của những thay đổi có thể xảy ra. Điều này cần nghiên cứu các xu hướng chính và thời gian về những thay đổi có thể xảy ra trong các xu hướng cũng như tư duy tưởng tượng về tương lai.

Những thay đổi được xem xét có thể bao gồm:

- thay đổi bên ngoài (chẳng hạn như thay đổi về công nghệ);

- các quyết định cần đưa ra trong tương lai gần nhưng có thể có nhiều kết quả;
- nhu cầu của bên liên quan và cách chúng có thể thay đổi;
- những thay đổi trong môi trường vĩ mô (chế định, nhân khẩu học, v.v...). Một số thay đổi sẽ chắc chắn xảy ra và một số sẽ không chắc chắn.

Đôi khi, một thay đổi có thể do hệ quả của rủi ro khác. Ví dụ, rủi ro về biến đổi khí hậu sẽ dẫn đến thay đổi trong yêu cầu tiêu dùng liên quan đến thực phẩm. Điều này sẽ ảnh hưởng đến các thực phẩm có thể được lợi nhuận xuất khẩu cũng như những thực phẩm có thể được trồng tại địa phương.

Các yếu tố cục bộ và vĩ mô hoặc những xu hướng có thể được liệt kê và được xếp hạng thành (1) quan trọng (2) không chắc chắn. Sự chú ý đặc biệt được tập trung vào những yếu tố quan trọng nhất và không chắc chắn nhất. Các yếu tố hoặc xu hướng chính được sắp xếp với nhau để hiển thị các khu vực trong đó các kịch bản có thể được xây dựng.

Một loạt các kịch bản được đề xuất trong đó mỗi kịch bản tập trung vào thay đổi hợp lý trong các thông số.

Tiếp theo, một "câu chuyện" được viết ra cho mỗi kịch bản nói về cách thức có thể di chuyển từ đây sang kịch bản có chủ đề. Những câu chuyện có thể bao gồm các chi tiết hợp lý làm tăng giá trị cho các kịch bản.

Sau đó các kịch bản có thể được sử dụng để thử nghiệm hoặc đánh giá câu hỏi ban đầu. Việc thử nghiệm tính đến bất kỳ yếu tố quan trọng nhưng có thể dự đoán được (ví dụ sử dụng mẫu) và sau đó tìm kiếm cách thức 'thành công' của chính sách (hoạt động) trong kịch bản mới này, và các kết quả "trước thử nghiệm" bằng cách sử dụng các câu hỏi 'điều gì - nếu' dựa trên những giả định mô hình.

Khi câu hỏi hoặc đề xuất được đánh giá với mỗi kịch bản, có thể rõ ràng rằng nó cần được sửa đổi để thiết thực hơn hoặc ít rủi ro hơn. Cũng cần có thể nhận biết một số các chỉ số dẫn dắt chỉ ra khi nào thay đổi xảy ra. Việc theo dõi và đáp ứng các chỉ số dẫn dắt có thể đưa ra cơ hội thay đổi trong các chiến lược được hoạch định.

Vì các kịch bản chỉ được xác định theo 'khoảng thời gian' trong tương lai có thể, nên quan trọng là phải đảm bảo đã tính đến xác suất xảy ra một kết quả cụ thể (kịch bản), nghĩa là chấp nhận một khuôn khổ rủi ro. Ví dụ khi các kịch bản trong trường hợp tốt nhất, trường hợp xấu nhất và trường hợp dự kiến được sử dụng, cần thực hiện nỗ lực nhất định để xác định phẩm chất hoặc thể hiện xác suất của từng kịch bản xảy ra.

B.10.5 Đầu ra

Có thể không có kịch bản thích hợp nhất nhưng một kịch bản nên kết thúc với cảm nhận rõ ràng hơn về phạm vi lựa chọn và cách thức thay đổi quá trình hành động được chọn khi yếu tố chỉ dẫn tiến triển.

B.10.6 Điểm mạnh và hạn chế

Phân tích kịch bản tính đến một phạm vi về tương lai có thể có mà có thể được ưa thích hơn cách tiếp cận truyền thống dựa vào dự báo cao-trung bình-thấp, thông qua việc sử dụng dữ liệu quá khứ, các

dự báo này giả định rằng các sự kiện tương lai sẽ có khả năng tiếp tục theo các xu hướng trong quá khứ. Đây là điều quan trọng đối với các kịch bản khi có rất ít kiến thức hiện tại về các vấn đề làm cơ sở cho những dự đoán hoặc khi những rủi ro đang được xem xét trong tương lai xa.

Tuy nhiên điểm mạnh này có một điểm yếu liên quan là khi có sự không chắc chắn cao một số kịch bản có thể không thực tế.

Những khó khăn chính trong việc sử dụng phân tích kịch bản liên quan tới sự sẵn có của dữ liệu và khả năng phân tích và người ra quyết định có thể xây dựng các kịch bản thực tế có thể phải chịu để điều tra các kết quả có thể.

Sự nguy hiểm của việc sử dụng phân tích kịch bản làm công cụ ra quyết định là các kịch bản được sử dụng có thể không có một cơ sở đầy đủ; dữ liệu có thể là suy đoán; và các kết quả không thực tế có thể không được thừa nhận như vậy.

B.11 Phân tích tác động kinh doanh (BIA)

B.11.1 Tổng quan

Phân tích tác động kinh doanh, cũng được biết đến như là đánh giá tác động kinh doanh, phân tích cách thức những rủi ro gián đoạn chính có thể ảnh hưởng đến các hoạt động của một tổ chức và nhận biết, lượng hóa các khả năng cần thiết để quản lý nó. Cụ thể, BIA đưa ra một sự hiểu biết thống nhất về:

- việc nhận biết và mức độ trọng yếu của các quá trình, chức năng kinh doanh chính và các nguồn lực liên quan và sự phụ thuộc lẫn nhau chính tồn tại đối với một tổ chức;
- cách thức các sự kiện gián đoạn sẽ tác động đến năng lực và khả năng đạt được các mục tiêu kinh doanh quan trọng;
- năng lực và khả năng cần thiết để quản lý tác động của một sự gián đoạn và khôi phục tổ chức ở mức độ hoạt động được thỏa thuận.

B.11.2 Sử dụng

BIA được sử dụng để xác định mức độ trọng yếu và khung thời gian khôi phục của các quá trình và nguồn lực liên quan (con người, thiết bị, công nghệ thông tin) để đảm bảo tiếp tục đạt được các mục tiêu. Ngoài ra, BIA hỗ trợ trong việc xác định sự phụ thuộc lẫn nhau và mối tương quan giữa các quá trình, các bên nội bộ và bên ngoài và mọi liên kết trong chuỗi cung ứng.

B.11.3 Đầu vào

Đầu vào bao gồm:

- một nhóm thực hiện phân tích và xây dựng kế hoạch;
- thông tin liên quan đến mục tiêu, môi trường, việc vận hành và sự phụ thuộc lẫn nhau của tổ chức;

- chi tiết về các hoạt động và vận hành của tổ chức, bao gồm các quá trình, các nguồn lực hỗ trợ, mối quan hệ với tổ chức khác, các sắp đặt thuê ngoài, các bên liên quan;
- các hệ quả tài chính và hoạt động do thiếu các quá trình quan trọng;
- bảng câu hỏi được chuẩn bị;
- danh sách những người được phỏng vấn từ các lĩnh vực liên quan của tổ chức và/hoặc các bên liên quan sẽ được liên lạc.

B.11.4 Quá trình

BIA có thể được thực hiện bằng cách sử dụng bảng câu hỏi, phỏng vấn, các hội thảo được cấu trúc hoặc kết hợp cả ba, để có được hiểu biết về các quá trình quan trọng, ảnh hưởng của việc thiếu những quá trình đó và khung thời gian khôi phục cần thiết và nguồn lực hỗ trợ.

Các bước chính bao gồm:

- dựa vào đánh giá rủi ro điểm yếu, xác nhận các quá trình và đầu ra chính của tổ chức để xác định mức độ trọng yếu của các quá trình;
- xác định hệ quả do sự gián đoạn trong các quá trình quan trọng được nhận biết về tài chính và/hoặc hoạt động, theo các khoảng thời gian xác định;
- nhận biết sự phụ thuộc lẫn nhau với các bên liên quan chính nội bộ và bên ngoài. Điều này có thể bao gồm việc lập sơ đồ đặc điểm của sự phụ thuộc lẫn nhau thông qua chuỗi cung ứng;
- xác định các nguồn lực sẵn có hiện tại và mức độ nguồn lực thiết yếu cần thiết để tiếp tục hoạt động ở một mức tối thiểu chấp nhận được sau một gián đoạn;
- nhận biết các chu trình công việc và các quá trình thay thế hiện đang sử dụng hoặc được hoạch định để xây dựng. Các chu trình công việc và quá trình thay thế có thể cần được xây dựng khi các nguồn lực hoặc năng lực không thể tiếp cận được hoặc không đầy đủ trong thời gian gián đoạn;
- xác định thời gian hỏng hóc tối thiểu có thể chấp nhận được (MAO) đối với mỗi quá trình dựa trên những hệ quả được nhận biết và các yếu tố thành công quan trọng cho chức năng đó. MAO đại diện cho khoảng thời gian tối đa tổ chức có thể gánh chịu về năng lực;
- xác định thời gian phục hồi (các) mục tiêu (RTO) đối với mọi thiết bị hoặc công nghệ thông tin chuyên môn hóa. RTO đại diện cho thời gian trong đó tổ chức nhằm mục đích khôi phục năng lực của thiết bị hoặc công nghệ thông tin chuyên môn;
- xác nhận mức độ chuẩn bị sẵn sàng hiện tại của các quá trình quan trọng để quản lý một sự gián đoạn. Điều này có thể bao gồm việc đánh giá mức độ dư thừa trong quá trình (ví dụ thiết bị dự phòng) hoặc có các nhà cung ứng thay thế.

B.11.5 Đầu ra

Các đầu ra như sau:

- một danh mục theo thứ tự ưu tiên các quá trình quan trọng và sự phụ thuộc lẫn nhau có liên quan;
- tác động về tài chính và vận hành được lập thành văn bản từ việc thiếu các quá trình quan trọng;
- các nguồn lực hỗ trợ cần thiết cho các quá trình quan trọng được nhận biết;
- khung thời gian ngừng sản xuất đối với quá trình quan trọng và khung thời gian khôi phục công nghệ thông tin liên quan.

B.11.6 Điểm mạnh và hạn chế

Điểm mạnh của BIA bao gồm:

- hiểu rõ các quá trình quan trọng mang lại cho tổ chức khả năng tiếp tục đạt được các mục tiêu đã tuyên bố của mình;
- hiểu rõ về các nguồn lực cần thiết;
- cơ hội xác định lại các quá trình vận hành của tổ chức để hỗ trợ khả năng thích ứng của tổ chức.

Hạn chế bao gồm:

- sự thiếu hiểu biết của những người tham gia liên quan trong việc hoàn thành bảng câu hỏi, tham gia cuộc phỏng vấn hoặc hội thảo;
- động lực của nhóm có thể ảnh hưởng đến việc phân tích hoàn chỉnh một quá trình quan trọng;
- những mong đợi đơn giản hoặc quá lạc quan của các yêu cầu khôi phục;
- sự khó khăn trong việc đạt được một mức độ hiểu biết đầy đủ về các hoạt động và vận hành của tổ chức.

B.12 Phân tích nguyên nhân gốc rễ (RCA)

B.12.1 Tổng quan

Việc phân tích một tổn thất lớn để ngăn ngừa sự tái diễn của nó thường được gọi là phân tích nguyên nhân gốc rễ (RCA), phân tích nguyên nhân gốc rễ của sai lỗi (RCFA) hoặc phân tích những thiệt hại. RCA tập trung vào những thiệt hại về tài sản do các loại sai lỗi khác nhau trong khi phân tích thiệt hại chủ yếu liên quan đến những thiệt hại về tài chính hoặc kinh tế do các yếu tố hoặc những biến cố bên ngoài. Phân tích này nỗ lực để nhận biết những nguyên nhân gốc rễ hoặc nguyên nhân ban đầu thay vì chỉ giải quyết những hiện tượng/triệu chứng thấy được tức thời. Phải thừa nhận rằng hành động khắc phục có thể không phải lúc nào cũng hoàn toàn hiệu lực và có thể cần việc cải tiến liên tục. RCA thường được áp dụng nhiều nhất đối với việc đánh giá mức độ của một thiệt hại chính nhưng cũng có thể được sử dụng để phân tích các thiệt hại trên cơ sở bao trùm hơn để xác định khi nào thực hiện cải tiến.

B.12.2 Sử dụng

RCA được áp dụng trong các bối cảnh khác nhau với những lĩnh vực sử dụng rộng như sau:

- RCA dựa trên sự an toàn được sử dụng cho việc điều tra tai nạn, an toàn và sức khỏe nghề nghiệp;
- phân tích sai lỗi được sử dụng trong các hệ thống công nghệ liên quan đến tính tin cậy và việc bảo trì;
- RCA dựa trên sản xuất được áp dụng trong lĩnh vực kiểm soát chất lượng đối với chế tạo công nghiệp;
- RCA dựa trên quá trình được tập trung vào các quá trình hoạt động;
- RCA dựa trên hệ thống đã được xây dựng là sự kết hợp của các lĩnh vực trên để giải quyết các hệ thống phức tạp ứng dụng trong quản lý thay đổi, quản lý rủi ro và phân tích hệ thống.

B.12.3 Đầu vào

Đầu vào cơ bản cho một RCA là tất cả các bằng chứng thu thập được từ sai lỗi hoặc tổn thất. Dữ liệu từ những sai lỗi tương tự khác cũng có thể được xem xét trong phân tích. Các đầu vào khác có thể là các kết quả được thực hiện để thử nghiệm các giả thuyết cụ thể.

B.12.4 Quá trình

Khi nhận biết được nhu cầu đối với một RCA, một nhóm các chuyên gia được chỉ định để thực hiện phân tích và lập ra các khuyến nghị. Loại chuyên gia hầu hết sẽ phụ thuộc vào chuyên môn cụ thể cần thiết để phân tích sai lỗi.

Mặc dù các phương pháp khác nhau có thể được sử dụng để thực hiện việc phân tích, nhưng các bước cơ bản trong triển khai một RCA đều tương tự và bao gồm:

- thành lập nhóm;
- thiết lập phạm vi và các mục tiêu của RCA;
- thu thập dữ liệu và bằng chứng từ những sai lỗi hoặc tổn thất;
- thực hiện một phân tích được cấu trúc để xác định nguyên nhân gốc rễ;
- xây dựng các giải pháp và lập ra các khuyến nghị;
- thực hiện các khuyến nghị;
- kiểm tra xác nhận sự thành công của các khuyến nghị được thực hiện.

Kỹ thuật phân tích có kết cấu có thể bao gồm một trong những nội dung sau:

- kỹ thuật "5 câu hỏi tại sao", nghĩa là hỏi lặp lại 'tại sao?' để lột bỏ các lớp nguyên nhân và nguyên nhân phụ);
- phân tích phương thức và tác động sai lỗi;
- Phân tích cây lỗi;

- biểu đồ Ishikawa hoặc xương cá;
- phân tích Pareto;
- sơ đồ nguyên nhân gốc rễ.

Việc đánh giá nguyên nhân thường tiến triển từ các nguyên nhân vật lý được thấy rõ ban đầu cho tới các nguyên nhân liên quan đến con người và cuối cùng là tập trung vào các nguyên nhân quản lý hoặc cơ bản. Các yếu tố nhân quả phải có thể được kiểm soát hoặc loại bỏ bởi các bên liên quan để hành động khắc phục có hiệu lực và xứng đáng.

B.12.5 Đầu ra

Đầu ra từ một RCA bao gồm:

- tài liệu về dữ liệu và bằng chứng được thu thập;
- các giả thuyết được xem xét;
- các kết luận về các nguyên nhân gốc rễ có khả năng xảy ra nhất đối với sai lỗi hoặc tổn thất;
- những khuyến nghị đối với hành động khắc phục.

B.12.6 Điểm mạnh và hạn chế

Điểm mạnh bao gồm:

- sự tham gia của các chuyên gia thích hợp làm việc trong môi trường nhóm;
- phân tích được cấu trúc;
- xem xét tất cả các giả thuyết có khả năng xảy ra;
- tài liệu về các kết quả;
- cần đưa ra các khuyến nghị cuối cùng.

Hạn chế của một RCA:

- các chuyên gia cần thiết có thể không sẵn có;
- bằng chứng quan trọng có thể bị hủy hoại do sai lỗi hoặc bị loại bỏ trong quá trình thu dọn;
- nhóm có thể không có đủ thời gian hoặc nguồn lực để đánh giá tình huống một cách đầy đủ;
- có thể không có khả năng thực hiện đầy đủ các khuyến nghị.

B.13 Phân tích phương thức và tác động của sai lỗi (FMEA), phân tích phương thức, tác động và mức độ nghiêm trọng của sai lỗi (FMECA)

B.13.1 Tổng quát

Phân tích phương thức và tác động của sai lỗi (FMEA) là kỹ thuật được dùng để nhận biết các cách thức trong đó các linh kiện, hệ thống hoặc quá trình có thể không thực hiện được mục đích thiết kế của chúng.

FMEA nhận biết:

- tất cả các phương thức sai lỗi tiềm ẩn của các bộ phận khác nhau trong hệ thống (phương thức sai lỗi là những gì được quan sát thấy mắc lỗi hoặc thực hiện không đúng);
- tác động của những sai lỗi này có thể có trên hệ thống;
- cơ chế sai lỗi;
- làm thế nào để tránh sai lỗi và/hoặc giảm nhẹ tác động của những sai lỗi lên hệ thống.

FMECA mở rộng FMEA để từng phương thức lỗi được nhận biết được xếp hạng theo tầm quan trọng hoặc mức nghiêm trọng của nó.

Phân tích mức độ nghiêm trọng thường định tính hoặc bán định lượng nhưng có thể được lượng hóa bằng cách sử dụng tỷ lệ sai lỗi thực tế.

B.13.2 Sử dụng

Có một vài ứng dụng của FMEA: FMEA thiết kế (hoặc sản phẩm) được sử dụng cho linh kiện hoặc các sản phẩm, FMEA hệ thống được sử dụng cho các hệ thống, FMEA quá trình được sử dụng cho quá trình chế tạo và lắp ráp, FMEA dịch vụ và FMEA phần mềm.

FMEA/FMECA có thể được áp dụng trong toàn bộ quá trình thiết kế, chế tạo hoặc vận hành một hệ thống vật lý.

Tuy nhiên, để nâng cao tính tin cậy, những thay đổi thường được áp dụng dễ dàng hơn ở giai đoạn thiết kế. FMEA và FMECA cũng có thể được ứng dụng cho các quá trình và thủ tục. Ví dụ, nó được sử dụng để nhận biết tiềm năng lỗi y học trong hệ thống chăm sóc sức khoẻ và sai lỗi trong duy trì các thủ tục.

FMEA/FMECA có thể được sử dụng để:

- hỗ trợ trong lựa chọn các phương án thay thế thiết kế với độ tin cậy cao;
- đảm bảo rằng tất cả phương thức sai lỗi của hệ thống và quá trình và các tác động của chúng tới thành công trong vận hành đều được xem xét;
- nhận biết phương thức sai lỗi của con người và các tác động;
- đưa ra cơ sở cho việc hoạch định thử nghiệm và bảo trì hệ thống vật lý;
- cải tiến việc thiết kế các thủ tục và quá trình

- cung cấp thông tin định tính hoặc định lượng cho kỹ thuật phân tích như phân tích cây lỗi.

FMEA và FMECA có thể cung cấp đầu vào cho các kỹ thuật phân tích khác như phân tích cây lỗi ở mức độ định lượng hay định tính.

B.13.3 Đầu vào

FMEA và FMECA cần thông tin đầy đủ, chi tiết về các yếu tố của hệ thống để việc phân tích có ý nghĩa về những cách thức trong đó mỗi yếu tố có thể mắc lỗi. Đối với một FMEA thiết kế chi tiết, yếu tố này có thể là ở mức độ linh kiện chi tiết riêng lẻ, trong khi đối với một FMEA hệ thống cấp cao hơn, các yếu tố có thể được xác định ở một mức độ cao hơn.

Thông tin có thể gồm:

- bản vẽ hoặc lưu đồ dòng chảy của hệ thống được phân tích và các thành tố của nó, hoặc các bước của một quá trình;
- hiểu biết về chức năng của từng bước trong quá trình hoặc thành tố của hệ thống;
- chi tiết các thông số môi trường và các thông số khác có thể ảnh hưởng đến vận hành;
- hiểu biết về các kết quả của sai lỗi cụ thể;
- thông tin quá khứ về sai lỗi gồm cả dữ liệu về tỉ lệ sai lỗi nếu có.

B.13.4 Quá trình

Quá trình FMEA như sau:

a) xác định phạm vi và mục tiêu của nghiên cứu;

b) tập hợp nhóm;

c) hiểu hệ thống/quá trình là đối tượng của FMECA;

d) chia hệ thống thành các bộ phận hoặc các bước;

e) xác định chức năng của từng bước hoặc từng bộ phận;

f) đối với từng bộ phận hoặc từng bước được liệt kê nhận biết:

   - cách thức từng phần có thể lỗi ?
   - cơ chế có thể sản sinh ra những phương thức sai lỗi này?
   - các tác động là gì nếu sai lỗi xảy ra?
   - sai lỗi là vô hại hoặc gây hại?
   - sai lỗi được phát hiện như thế nào?

g) nhận biết các điều khoản cố hữu trong thiết kế để bù đắp cho sai lỗi.

Đối với FMECA, nhóm nghiên cứu tiếp tục phân loại từng phương thức sai lỗi được nhận biết theo mức độ nghiêm trọng của nó.

Có một số cách có thể thực hiện điều này. Phương pháp phổ biến gồm:

- chỉ số mức rủi ro;
- mức rủi ro;
- số thứ tự rủi ro.

Mức độ nghiêm trọng của phương thức là một thước đo xác suất mà phương thức được coi là sẽ dẫn đến sai lỗi cho toàn bộ hệ thống, nó được định nghĩa là:

Xác suất tác động của sai lỗi x Tỉ lệ sai lỗi của phương thức x Thời gian vận hành của hệ thống

Nó thường được áp dụng cho sai lỗi thiết bị trong đó mỗi thuật ngữ trên có thể được xác định một cách định lượng và tất cả các phương thức sai lỗi đều có cùng một hệ quả.

Mức rủi ro có được bằng cách kết hợp các hệ quả của phương thức sai lỗi xảy ra với xác suất sai lỗi. Nó được sử dụng khi hệ quả của các phương thức sai lỗi khác nhau là khác nhau và có thể được áp dụng cho các hệ thống thiết bị hoặc quá trình. Mức rủi ro có thể được thể hiện một cách định tính, bán định lượng hoặc định lượng.

Số thứ tự rủi ro (RPN) là thước đo bán định lượng của mức độ nghiêm trọng thu được bằng việc nhân các số (thường từ 1 đến 10) đối với hệ quả của sai lỗi, khả năng xảy ra sai lỗi và khả năng phát hiện vấn đề. (Một sai lỗi được cho thứ tự cao hơn nếu nó khó phát hiện). Phương pháp này thường được sử dụng nhiều nhất trong các ứng dụng đảm bảo chất lượng.

Khi phương thức và cơ chế sai lỗi được nhận biết, hành động khắc phục có thể được xác định và thực hiện đối với phương thức sai lỗi nghiêm trọng hơn.

FMEA được lập thành văn bản trong báo cáo gồm:

- chi tiết về hệ thống đã được phân tích;
- các thức thực hành đã được thực hiện;
- giả định được lập trong phân tích;
- nguồn dữ liệu;
- các kết quả, gồm cả bảng tính hoàn chỉnh;
- mức độ nghiêm trọng (nếu hoàn thành) và phương pháp được sử dụng để xác định;
- mọi khuyến nghị phân tích thêm, thay đổi thiết kế hoặc các đặc trưng được kết hợp trong kế hoạch thử nghiệm, v.v...

Hệ thống có thể được đánh giá lại theo một chu kỳ FMEA khác sau khi những hành động đã được hoàn thành.

B.13.5 Đầu ra

Đầu ra sơ bộ của FMEA là danh mục phương thức sai lỗi, cơ chế sai lỗi và các tác động đối với mỗi thành phần hoặc giai đoạn của hệ thống hay quá trình (có thể bao gồm thông tin khả năng sai lỗi). Thông tin cũng được đưa ra về nguyên nhân của sai lỗi và các hệ quả cho toàn bộ hệ thống. Đầu ra từ FMECA gồm xếp hạng quan trọng dựa trên khả năng xảy ra hệ thống sẽ mắc lỗi, mức rủi ro từ phương thức sai lỗi hoặc một sự kết hợp giữa mức rủi ro và "khả năng phát hiện" phương thức sai lỗi.

FMECA có thể đưa ra một kết quả định lượng nếu dữ liệu về tỷ lệ sai lỗi phù hợp và hệ quả định lượng được sử dụng.

B.13.6 Điểm mạnh và hạn chế

Điểm mạnh của FMEA/FMECA như sau:

- áp dụng rộng rãi đối với các phương thức sai lỗi của con người, thiết bị và hệ thống và đối với phần cứng, phần mềm và các thủ tục;
- nhận biết các phương thức sai lỗi thành phần, nguyên nhân và tác động của chúng lên hệ thống và thể hiện chúng theo một định dạng có thể đọc được dễ dàng;
- tránh nhu cầu sửa đổi thiết bị tốn kém khi đang sử dụng bằng cách nhận biết sớm các vấn đề trong quá trình thiết kế;
- nhận biết các phương thức sai lỗi tại một điểm và các yêu cầu đối với việc hệ thống dự phòng hoặc an toàn;
- cung cấp đầu vào cho việc xây dựng các chương trình theo dõi bằng cách làm nổi bật tính năng chính được theo dõi.

Hạn chế bao gồm:

- chúng chỉ có thể được sử dụng để nhận biết các phương thức sai lỗi duy nhất, chứ không phải sự kết hợp các phương thức sai lỗi;
- trừ khi được kiểm soát và được chú trọng thỏa đáng những nghiên cứu này có thể tốn thời gian và chi phí;
- chúng có thể khó và gây mệt mỏi đối với các hệ thống nhiều lớp phức tạp.

B.13.7 Tài liệu tham khảo

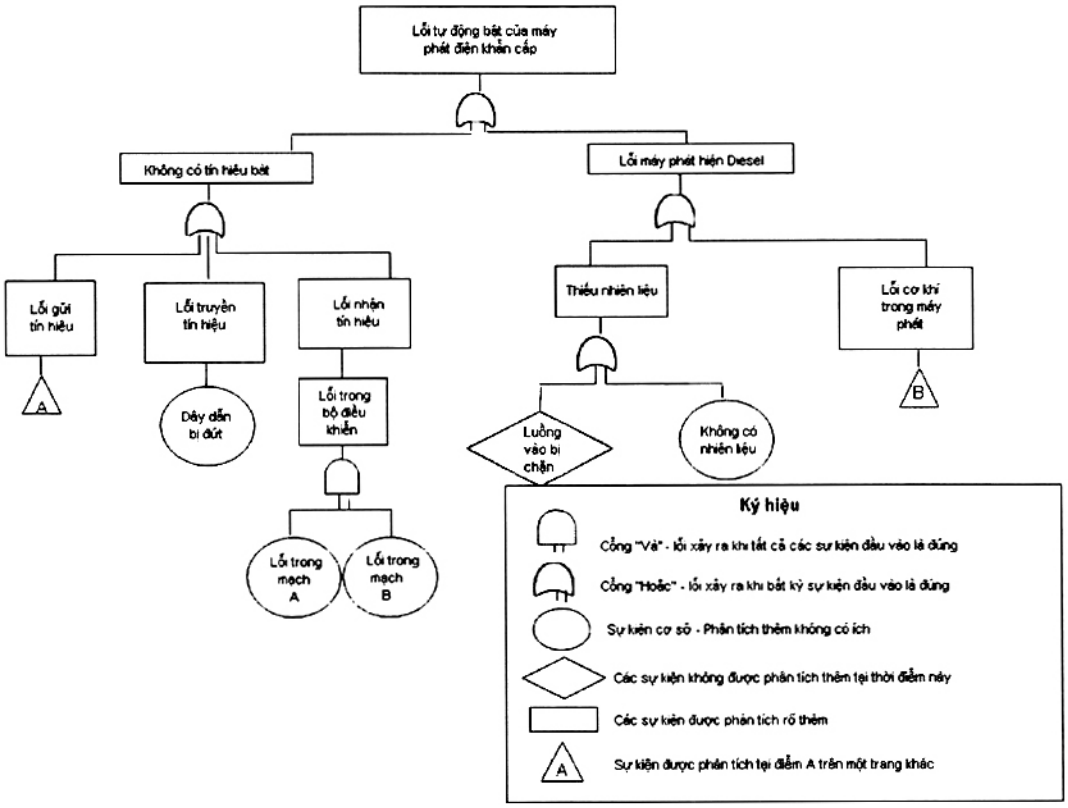
IEC 60812, Kỹ thuật phân tích sự tin cậy của hệ thống – Quy trình phân tích và phương thức tác động sai lỗi (FMEA).

B.14 Phân tích cây lỗi (FTA)

B.14.1 Tổng quát

FTA là một kỹ thuật để nhận biết và phân tích các yếu tố có thể đóng góp vào một sự kiện không mong muốn quy định (được gọi là "sự kiện đầu"). Yếu tố nguyên nhân được nhận biết, được tổ chức theo suy luận một cách hợp lý và được thể hiện bằng hình ảnh trong một sơ đồ hình cây mô tả các yếu tố nguyên nhân và mối quan hệ hợp lý của chúng với sự kiện đầu.

Các yếu tố được nhận biết trong cây có thể là những sự kiện liên quan đến các sai lỗi phần cứng thành phần, lỗi con người hoặc bất kỳ sự kiện thích hợp nào khác dẫn đến sự kiện không mong muốn.



Hình B.2 – Ví dụ về một FTA từ IEC 60300-3-9

B.14.2 Sử dụng

Cây lỗi có thể được sử dụng một cách định tính để nhận biết các nguyên nhân tiềm ẩn và đường dẫn đến một sai lỗi (sự kiện đầu) hoặc một cách định lượng để tính toán xác suất của sự kiện đầu, giả sử đã biết xác suất của các biến cố nguyên nhân.

Nó có thể được sử dụng ở giai đoạn thiết kế của hệ thống để nhận biết nguyên nhân sai lỗi tiềm ẩn và từ đó lựa chọn những phương án thiết kế khác nhau. Nó có thể được sử dụng ở giai đoạn vận hành để

nhận biết cách thức những sai lỗi nghiêm trọng có thể xảy ra và tầm quan trọng tương đối của đường dẫn tới sự kiện trên cùng. Cây lỗi cũng có thể được sử dụng để phân tích một sai lỗi đã xảy ra để biểu diễn theo biểu đồ cách thức sự kiện khác nhau cùng là nguyên nhân gây ra sai lỗi.

B.14.3 Đầu vào

Đối với phân tích định tính, hiểu biết về hệ thống và nguyên nhân sai lỗi là cần thiết, cũng như hiểu biết kỹ thuật về cách thức hệ thống có thể mắc lỗi. Biểu đồ chi tiết là hữu ích để hỗ trợ phân tích.

Đối với phân tích định lượng, dữ liệu về tỷ lệ sai lỗi hoặc xác suất nằm trong trạng thái bị lỗi đối với tất cả các sự kiện cơ bản trong cây lỗi là cần thiết.

B.14.4 Quá trình

Các bước xây dựng cây lỗi như sau:

- Nhận biết sự kiện đầu được phân tích. Đây có thể là sai lỗi hoặc có thể là kết quả rộng hơn của sai lỗi đó. Nếu kết quả được phân tích, cây này có thể bao gồm một phần liên quan đến việc giảm nhẹ sai lỗi thực tế.
- Bắt đầu với sự kiện đầu, các nguyên nhân trung gian có thể có hoặc phương thức sai lỗi dẫn đến sự kiện đầu được nhận biết.
- Từng nguyên nhân phương thức sai lỗi này được phân tích để nhận biết cách thức sai lỗi bị gây ra.
- Việc nhận biết từng bước vận hành hệ thống không mong muốn được nối tiếp các cấp hệ thống thấp hơn liên tiếp cho đến khi phân tích sâu hơn trở lên không hiệu quả. Trong hệ thống phần cứng đây có thể là cấp sai lỗi thành phần. Các sự kiện và yếu tố nguyên nhân ở cấp hệ thống thấp nhất được phân tích được coi là các sự kiện cơ sở.
- Nếu khả năng có thể được ấn định cho các sự kiện cơ sở, có thể tính toán khả năng của sự kiện đầu. Để việc lượng hóa có ý nghĩa, phải có thể chỉ ra rằng ở mọi cổng, tất cả các đầu vào đều cần thiết và đủ để đưa ra biến cố đầu ra. Nếu tình huống không phải như vậy, cây lỗi không có giá trị đối với phân tích khả năng nhưng có thể là một công cụ hữu ích đối với việc thể hiện mối quan hệ nhân quả.

Khi một phần trong việc lượng hóa cây lỗi có thể cần được đơn giản hóa bằng cách sử dụng đại số Boolean để tính toán phương thức sai lỗi trùng lặp.

Cũng như việc đưa ra ước lượng về khả năng của sự kiện đầu, tập hợp các điểm giao cắt ít nhất tạo thành các lộ trình riêng biệt đến sự kiện đầu có thể được nhận biết và ảnh hưởng của chúng tới sự kiện đầu được tính toán.

Trừ các cây lỗi đơn giản, gói phần mềm là cần thiết để xử lý đúng đắn các tính toán khi sự kiện được lặp đi lặp lại có mặt ở nhiều nơi trong cây lỗi và để tính toán tập hợp các điểm giao cắt ít nhất. Các công cụ phần mềm giúp đảm bảo tính nhất quán, tính đúng đắn và khả năng kiểm tra xác nhận.

B.14.5 Đầu ra

Đầu ra từ phân tích cây lỗi như sau:

- thể hiện bằng hình ảnh cách thức biến cố đều có thể xảy ra trong đó chỉ ra các lộ trình tương tác tại đó hai hoặc nhiều sự kiện đồng thời phải xảy ra;
- một danh mục tập hợp các điểm giao cắt ít nhất (các lộ trình sai lỗi riêng lẻ) với khả năng mà từng tập hợp sẽ xảy ra (nếu sẵn có dữ liệu);
- xác suất của sự kiện đầu.

B.14.6 Điểm mạnh và hạn chế

Điểm mạnh của FTA:

- bắt buộc một cách tiếp cận có kỷ luật, có tính hệ thống cao, nhưng đồng thời cũng đủ linh hoạt để cho phép phân tích một loạt các yếu tố, bao gồm sự tương tác của con người và hiện tượng vật lý.
- ứng dụng cách tiếp cận "từ trên xuống", hàm ý trong kỹ thuật, tập trung sự chú ý vào những tác động của sai lỗi liên quan trực tiếp đến sự kiện đầu.
- FTA đặc biệt hữu ích đối với các hệ thống phân tích với nhiều điểm tương giao và sự tương tác.
- việc thể hiện bằng hình ảnh tạo sự dễ hiểu về tính năng của hệ thống và các yếu tố trong hệ thống, nhưng vì cây thường lớn, nên việc xử lý cây lỗi có thể yêu cầu các hệ thống máy tính. Đặc trưng này cho phép đưa vào các mối quan hệ hợp lý phức tạp hơn (ví dụ NAND và NOR) nhưng cũng làm cho việc kiểm tra xác nhận cây lỗi khó khăn.
- phân tích hợp lý cây lỗi và nhận biết các tập hợp các điểm giao cắt ít nhất là hữu ích trong việc nhận biết những lộ trình sai lỗi đơn giản trong một hệ thống rất phức tạp trong đó sự kết hợp cụ thể sự kiện dẫn đến sự kiện đầu có thể bị bỏ qua.

Hạn chế bao gồm:

- sự không chắc chắn về khả năng xảy ra của các sự kiện cơ sở được đưa vào tính toán xác suất của sự kiện đầu. Điều này có thể dẫn đến độ không đảm bảo cao khi khả năng xảy ra sai lỗi của sự kiện đầu không được biết chính xác; tuy nhiên, vẫn có thể có một mức độ tin cậy cao trong một hệ thống được hiểu rõ.
- trong một số tình huống, các sự kiện nguyên nhân không ràng buộc nhau và nó có thể khó khăn để xác định xem tất cả các lộ trình quan trọng đến sự kiện đầu có được đưa vào. Ví dụ, đưa tất cả các nguồn gây cháy vào một phân tích về hỏa hoạn là sự kiện đầu. Trong tình huống này, không thể phân tích xác suất.
- cây lỗi là một mô hình tĩnh; sự phụ thuộc lẫn nhau về thời gian không được đề cập.
- cây lỗi chỉ có thể xử lý trạng thái hai thành phần (sai lỗi/không sai lỗi).

- vì phương thức lỗi con người có thể được nêu trong một cây lỗi định tính, nên nhìn chung những sai lỗi về mức độ hoặc chất lượng đặc trưng cho lỗi con người không thể dễ dàng đưa vào.
- một cây lỗi không cho phép những tác động dây chuyền hoặc những sai lỗi có điều kiện được đưa vào một cách dễ dàng.

B.14.7 Tài liệu tham khảo

IEC 61025, Phân tích cây lỗi (FTA);

IEC 60300- 3-9, Quản lý tính tin cậy – Phần 3: Hướng dẫn áp dụng – Mục 9: Phân tích rủi ro của các hệ thống công nghệ.

B.15 Phân tích cây sự kiện (ETA)

B.15.1 Tổng quan

ETA là một kỹ thuật đồ thị về thể hiện chuỗi các sự kiện loại trừ lẫn nhau theo một sự kiện khởi đầu phù hợp với việc thực hiện/không thực hiện chức năng của các hệ thống khác nhau được thiết kế để giảm nhẹ hệ quả của nó (xem Hình B.3). Nó có thể được áp dụng một cách định tính và định lượng.

Hình B.3 cho thấy những tính toán đơn giản đối với một cây sự kiện mẫu, trong đó các nhánh là hoàn toàn độc lập.

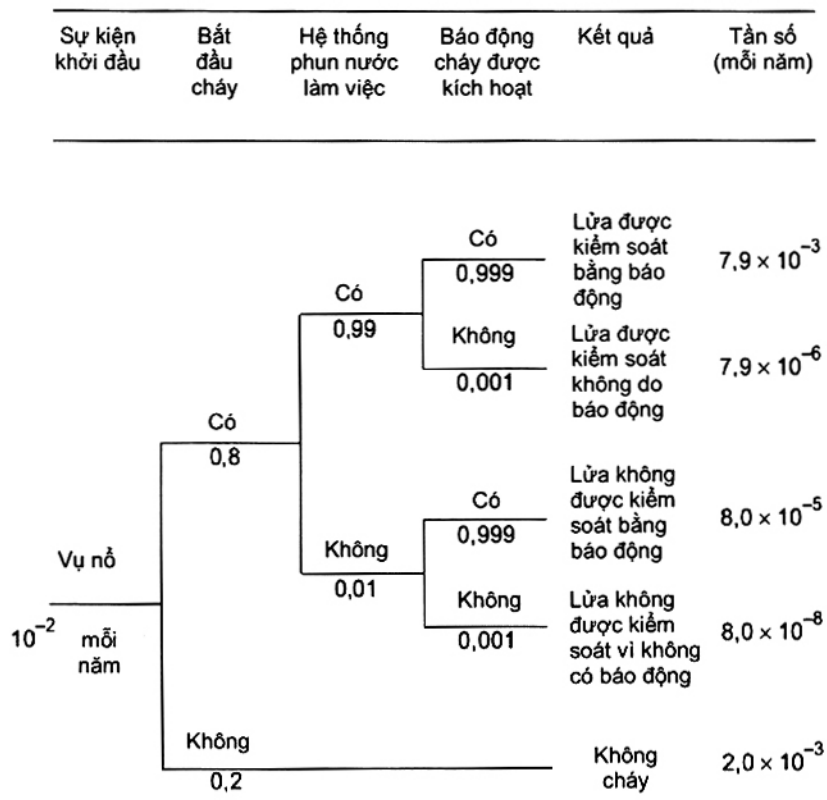
Nhờ biểu diễn ở dạng cây, ETA là có thể thể hiện các sự kiện làm xấu thêm hoặc giảm nhẹ sự kiện trong phản ứng tới sự kiện ban đầu, có tính đến các hệ thống, chức năng hoặc các rào cản bổ sung.

B.15.2 Sử dụng

ETA có thể được sử dụng để mô hình hóa, tính toán và xếp hạng (từ một quan điểm về rủi ro) tình huống tai nạn khác nhau.

ETA có thể được sử dụng ở bất cứ giai đoạn nào trong vòng đời sản phẩm hoặc quá trình. Nó có thể được sử dụng một cách định tính để hỗ trợ tình huống tiềm ẩn động não tập thể và chuỗi các sự kiện tiếp theo sự kiện khởi đầu và cách thức các kết quả bị tác động bởi biện pháp xử lý khác nhau, các rào cản hoặc kiểm soát nhằm giảm nhẹ các kết quả không mong muốn.

Phân tích định lượng đưa vào để xem xét khả năng chấp nhận các kiểm soát. Nó thường được sử dụng nhiều nhất đối với các sai lỗi theo mô hình trong đó có nhiều biện pháp bảo vệ.



Hình B.3 – Ví dụ về cây sự kiện

ETA có thể được sử dụng để mô hình hóa các sự kiện khởi đầu có thể mang lại tổn thất hoặc lợi ích. Tuy nhiên, các trường hợp trong đó lộ trình tối ưu hóa lợi ích được theo đuổi được mô hình hóa thường xuyên hơn bằng cách sử dụng cây quyết định.

B.15.3 Đầu vào

Đầu vào bao gồm:

- một danh mục các sự kiện khởi đầu thích hợp;
- thông tin về cách xử lý, các rào cản và kiểm soát, và khả năng sai lỗi của chúng (đối với phân tích định lượng);
- hiểu biết về các quá trình theo đó phát triển sai lỗi ban đầu.

B.15.4 Quá trình

Một cây sự kiện bắt đầu bằng việc lựa chọn một sự kiện khởi đầu. Đây có thể là một tai nạn như là nổ bụi hoặc sự kiện nguyên nhân chẳng hạn như một sai lỗi về công suất. Sau đó các chức năng hoặc hệ thống đặt ra để giảm nhẹ các kết quả được liệt kê theo thứ tự. Đối với mỗi chức năng hoặc hệ thống, vẽ một đường thể hiện sự thành công hay thất bại của chúng. Xác suất sai lỗi cụ thể có thể được ấn định

cho từng đường, xác suất có điều kiện này được ước lượng, ví dụ như theo đánh giá của chuyên gia hoặc phân tích cây lỗi. Theo cách này, các lộ trình khác nhau từ biến cố khởi đầu được mô hình hóa.

Lưu ý rằng các khả năng xảy ra trên cây sự kiện là xác suất có điều kiện, ví dụ xác suất về sự hoạt động của vòi phun nước không phải là xác suất có được từ các thử nghiệm dưới điều kiện thông thường, mà là xác suất hoạt động trong điều kiện hỏa hoạn gây ra bởi một vụ nổ.

Mỗi lộ trình thông qua cây thể hiện xác suất mà tất cả các xác suất trong lộ trình đó sẽ xảy ra. Vì vậy, tần số của kết quả được thể hiện bằng sản phẩm của xác suất có điều kiện riêng lẻ và tần suất của xác suất khởi đầu, giả sử, các sự kiện khác nhau là độc lập.

B.15.5 Đầu ra

Đầu ra từ ETA bao gồm:

- mô tả định tính các vấn đề tiềm ẩn như sự kết hợp các sự kiện dẫn đến các loại vấn đề khác nhau (dải kết quả) từ các sự kiện khởi đầu;
- các ước lượng định lượng tần số sự kiện hoặc xác suất và tầm quan trọng tương đối của chuỗi sai lỗi khác nhau và các sự kiện thành phần;
- danh mục khuyến nghị để giảm rủi ro;
- đánh giá định lượng hiệu lực của khuyến nghị.

B.15.6 Điểm mạnh và hạn chế

Điểm mạnh của ETA bao gồm:

- ETA hiển thị các tình huống tiềm ẩn tiếp theo sự kiện khởi đầu, được phân tích ảnh hưởng của sự thành công hoặc sai lỗi trong việc giảm nhẹ hệ thống hoặc chức năng theo một sơ đồ rõ ràng;
- nó tính đến thời gian, sự phụ thuộc và các tác động dây chuyền cồng kềnh để lập mô hình trong cây lỗi;
- nó thể hiện bằng đồ thị chuỗi sự kiện không thể thể hiện khi sử dụng cây lỗi.

Hạn chế bao gồm:

- để sử dụng ETA như là một phần của việc đánh giá một cách toàn diện, cần nhận biết tất cả các sự kiện khởi đầu tiềm ẩn. Điều này có thể được thực hiện bằng cách sử dụng phương pháp phân tích khác (ví dụ HAZOP, PHA), tuy nhiên, luôn tiềm ẩn đối với việc các sự kiện khởi đầu quan trọng bị thiếu.
- với cây sự kiện, chỉ những trạng thái thành công hay sai lỗi của hệ thống được xử lý và khó để kết hợp thành công hoặc sự kiện phục hồi;
- mọi lộ trình đều có điều kiện là sự kiện đã xảy ra tại các điểm rẽ nhánh trước đó trên lộ trình. Do đó, nhiều sự phụ thuộc dọc theo các lộ trình có thể có được đề cập. Tuy nhiên, một số sự phụ thuộc, như các thành phần chung, các hệ thống hữu dụng và người vận hành, có thể bị bỏ qua nếu không được xử lý cẩn thận, điều này có thể dẫn đến việc các ước lượng lạc quan về rủi ro.

B.16 Phân tích nguyên nhân – hệ quả

B.16.1 Khái quát

Phân tích nguyên nhân – hệ quả là sự kết hợp phân tích cây lỗi và cây sự kiện. Nó bắt đầu từ một sự kiện quan trọng và phân tích các hệ quả bằng phương pháp kết hợp các cổng logic CÓ/KHÔNG thể hiện điều kiện có thể xảy ra hoặc sai lỗi của hệ thống được thiết kế để giảm nhẹ hệ quả của sự kiện khởi đầu. Nguyên nhân của các điều kiện hoặc các sai lỗi được phân tích theo cây lỗi (xem B.15).

B.16.2 Cách sử dụng

Ban đầu, phân tích nhân quả được xây dựng như một công cụ đáng tin cậy cho các hệ thống an toàn quan trọng nhằm đưa ra hiểu biết đầy đủ hơn về các sai lỗi hệ thống. Giống với phân tích cây lỗi, nó được sử dụng để thể hiện nguyên lý sai lỗi dẫn đến một sự kiện quan trọng, nhưng nó bổ sung thêm chức năng cho cây lỗi bằng cách cho phép sai lỗi liên tiếp theo thời gian được phân tích. Phương pháp này cũng cho phép sự chậm trễ về thời gian được đưa vào phân tích hệ quả, điều mà cây sự kiện không làm được.

Phương pháp này được sử dụng để phân tích các lộ trình khác nhau một hệ thống có thể thực hiện theo một sự kiện quan trọng và phụ thuộc vào cách hoạt động của các hệ thống phụ cụ thể (chẳng hạn như các hệ thống ứng phó khẩn cấp). Nếu được lượng hóa chúng sẽ đưa ra một ước lượng về xác suất của các hệ quả khác nhau có thể có tiếp theo một sự kiện quan trọng.

Nếu từng chuỗi trong một biểu đồ nhân – quả là sự kết hợp của các nhánh lỗi, thì phân tích nhân quả có thể được sử dụng làm công cụ để xây dựng cây lỗi lớn.

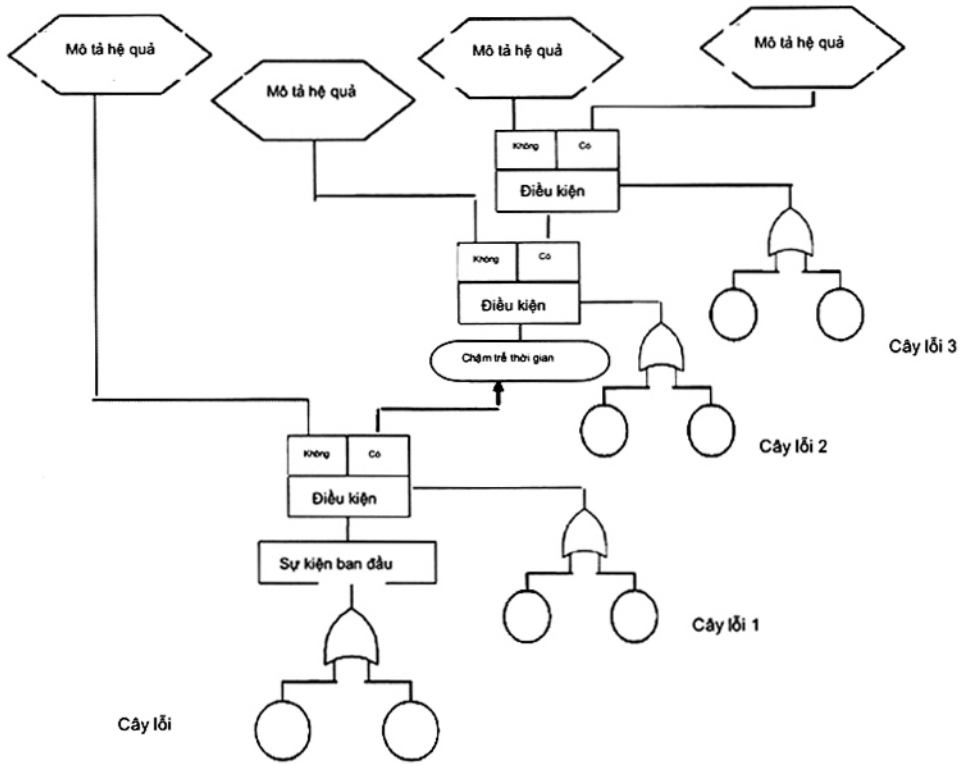
Các biểu đồ rất phức tạp để đưa ra và sử dụng và nhằm được sử dụng khi mức độ của các hệ quả tiềm ẩn do sai lỗi biện minh cho nỗ lực cao độ.

B.16.3 Đầu vào

Đòi hỏi sự hiểu biết về hệ thống và phương thức sai lỗi của hệ thống và các tình huống sai lỗi.

B.16.4 Quá trình

Hình B.4 thể hiện sơ đồ khái niệm về một phân tích nguyên nhân – hệ quả điển hình.



Hình B.4 – Ví dụ về phân tích nguyên nhân hệ quả

Quy trình như sau:

a) Nhận biết sự kiện quan trong (hoặc sự kiện ban đầu) (tương đương với sự kiện đầu của cây lỗi và sự kiện đầu của cây sự kiện).

b) Xây dựng và xác nhận giá trị cây lỗi đối với các nguyên nhân của sự kiện ban đầu được mô tả ở B.14. Các ký hiệu được sử dụng như trong phân tích cây lỗi thông thường.

c) Quyết định thứ tự trong đó các điều kiện được xem xét. Đây cần là một trình tự hợp lý như trình tự thời gian chúng xảy ra.

d) Xây dựng các lộ trình cho các hệ quả theo các điều kiện khác nhau. Điều này tương tự như cây sự kiện nhưng chia các lộ trình của cây sự kiện như được biểu diễn bằng ô vuông được gắn với điều kiện áp dụng cụ thể.

e) Giả sử các sai lỗi đối với từng ô điều kiện là độc lập có thể tính toán xác suất của từng hệ quả. Đầu tiên, điều này đạt được bởi việc ấn định xác suất cho mỗi đầu ra của ô điều kiện (sử dụng cây lỗi liên quan khi thích hợp). Xác suất của một chuỗi bất kỳ dẫn đến một hệ quả cụ thể đạt được bằng cách nhân xác suất của từng chuỗi điều kiện chấm dứt ở hệ quả cụ thể. Nếu có nhiều hơn một chuỗi kết thúc tại cùng một hệ quả, xác suất của từng chuỗi được cộng lại. Nếu có sự phụ

thuộc giữa các sai lỗi điều kiện trong chuỗi (ví dụ một sai lỗi về công suất có thể gây ra một số điều kiện sai lỗi) thì sự phụ thuộc này cần được giải quyết trước khi tính toán.

B.16.5 Đầu ra

Đầu ra của phân tích nhân – quả là sự biểu diễn bằng sơ đồ về cách thức hệ thống có thể mắc sai lỗi trong đó thể hiện cả nguyên nhân và hệ quả. Một ước lượng xác suất xảy ra của từng hệ quả tiềm ẩn được dựa vào phân tích xác suất xuất hiện các điều kiện cụ thể tiếp theo sự kiện quan trọng.

B.16.6 Điểm mạnh và hạn chế

Những thuận lợi của phân tích nhân quả tương tự như những thuận lợi của cây sự kiện và cây lỗi được kết hợp. Ngoài ra, nó vượt qua một số giới hạn của những kỹ thuật đó bằng khả năng phân tích các sự kiện tiến triển theo thời gian. Phân tích nhân quả đưa ra một một cái nhìn toàn diện về hệ thống.

Những hạn chế phức tạp hơn phân tích cây lỗi và phân tích cây sự kiện, trong cả việc xây dựng và cách thức xử lý sự phụ thuộc trong quá trình lượng hóa.

B.17 Phân tích nguyên nhân và tác động

B.17.1 Tổng quan

Phân tích nguyên nhân và tác động là một phương pháp được cấu trúc để nhận biết các nguyên nhân có thể của một sự kiện hoặc vấn đề không mong muốn. Nó sắp xếp các yếu tố đóng góp có thể có thành nhiều loại để tất cả các giả thuyết đều có thể được xem xét. Tuy nhiên, nó không tự chỉ ra các nguyên nhân thực tế, vì những nguyên nhân này chỉ có thể được xác định bởi bằng chứng thực tế và thử nghiệm thực nghiệm giả thuyết. Thông tin được sắp xếp trong một biểu đồ xương cá (cũng được gọi là Ishikawa) hoặc đôi khi trong biểu đồ hình cây (xem B.17.4)

B.17.2 Sử dụng

Phân tích nguyên nhân và tác động đưa ra hiển thị bằng hình ảnh được cấu trúc về một danh mục các nguyên nhân do một tác động cụ thể. Tác động này có thể là tích cực (một mục tiêu) hay tiêu cực (một vấn đề) tùy vào bối cảnh.

Phân tích này được sử dụng để cho phép xem xét tất cả các tình huống và nguyên nhân có thể có được thực hiện bởi một nhóm các chuyên gia và cho phép sự đồng thuận được thiết lập với phần lớn các nguyên nhân có thể xảy ra sau đó có thể được kiểm tra bằng thực nghiệm hoặc đánh giá dữ liệu sẵn có. Nó có giá trị nhất vào lúc bắt đầu phân tích để mở rộng tư duy về các nguyên nhân có thể và sau đó thiết lập các giả thuyết tiềm ẩn có thể được coi là chính thức hơn.

Xây dựng một biểu đồ nguyên nhân và tác động có thể được thực hiện khi có nhu cầu:

- nhận biết nguyên nhân gốc rễ có thể có, những lý do cơ bản, đối với một tác động, vấn đề hoặc điều kiện cụ thể;

- sắp xếp và liên kết một số tương tác giữa các yếu tố tác động đến một quá trình cụ thể;
- phân tích các vấn đề hiện tại để hành động khắc phục có thể được thực hiện.

Lợi ích từ việc xây dựng một biểu đồ nguyên nhân và tác động bao gồm:

- tập trung sự chú ý của các thành viên xem xét về một vấn đề cụ thể;
- giúp xác định nguyên nhân gốc của một vấn đề bằng cách sử dụng phương pháp tiếp cận có cấu trúc;
- khuyến khích sự tham gia nhóm và vận dụng kiến thức của nhóm đối với sản phẩm hay quá trình;
- sử dụng một định dạng ngắn gọn, dễ đọc để lập biểu đồ các mối quan hệ nguyên nhân và tác động;
- chỉ ra nguyên nhân có thể có của sự biến động trong quá trình;
- nhận biết các khu vực tại đó dữ liệu cần được thu thập cho việc nghiên cứu thêm.

Có thể sử dụng phân tích nguyên nhân và thay đổi như một phương pháp trong thực hiện phân tích nguyên nhân gốc rễ (xem B.12).

B.17.3 Đầu vào

Đầu vào đối cho phân tích nguyên nhân và tác động có thể có từ kiến thức chuyên môn và kinh nghiệm của những người tham gia hay một mô hình đã được xây dựng và sử dụng trước đó.

B.17.4 Quá trình

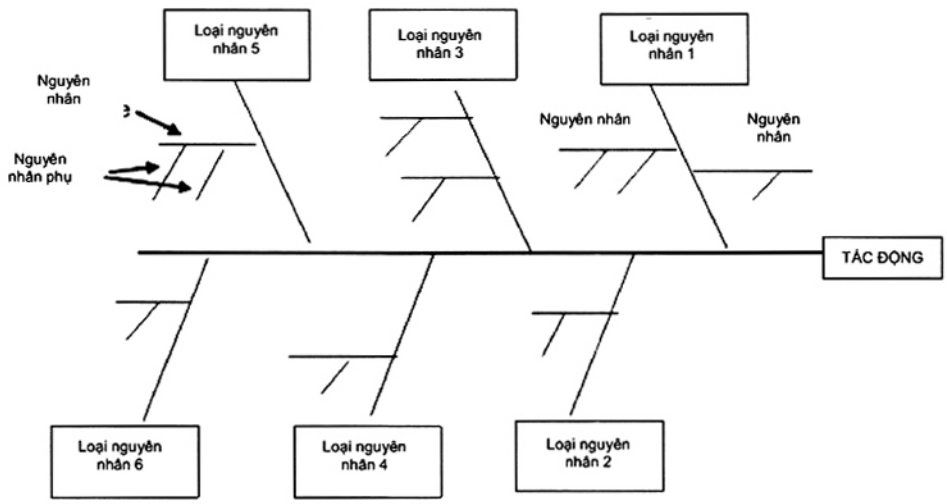
Phân tích nguyên nhân và tác động cần được thực hiện bởi một nhóm chuyên gia có kiến thức về vấn đề cần giải pháp.

Các bước cơ bản trong thực hiện phân tích nguyên nhân và kết quả là:

- thiết lập tác động được phân tích và đặt vào một ô. Tác động có thể là tích cực (một mục tiêu) hoặc tiêu cực (một vấn đề) tùy vào các trường hợp.
- xác định loại nguyên nhân chính được thể hiện ở các ô trong biểu đồ xương cá. Thông thường, đối với một vấn đề của hệ thống, các loại này có thể là con người, thiết bị, môi trường, quá trình, v.v...Tuy nhiên, chúng được lựa chọn phù hợp với bối cảnh cụ thể;
- điền các nguyên nhân có thể đối với mỗi loại chính vào các nhánh và nhánh con để mô tả mối quan hệ giữa chúng;
- tiếp tục đặt câu hỏi "tại sao?" hoặc "điều gì gây ra?" để kết nối các nguyên nhân;
- xem xét tất cả các nhánh để xác nhận tính nhất quán và đầy đủ và đảm bảo rằng nguyên nhân áp dụng cho tác động chính;
- nhận biết các nguyên nhân có khả năng xảy ra nhất được dựa vào ý kiến của nhóm và bằng chứng

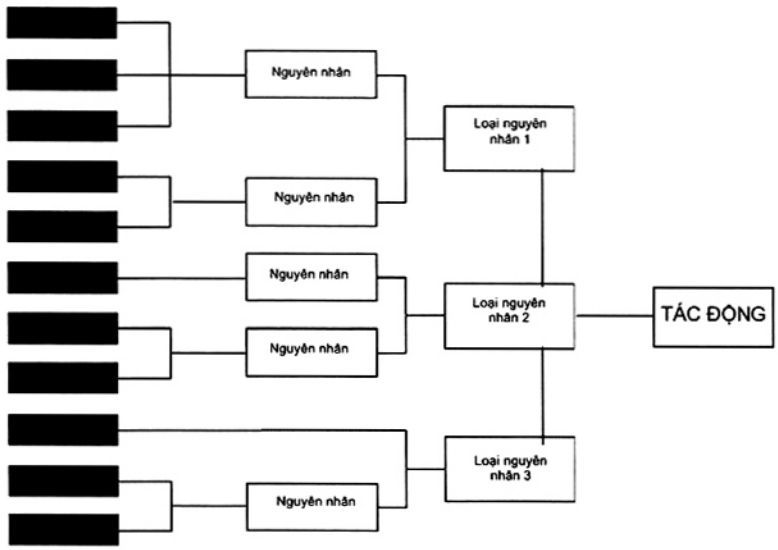
sẵn có.

Các kết quả thường được hiển thị theo biểu đồ xương cá hay Ishikawa hoặc biểu đồ hình cây. Biểu đồ xương cá được cấu trúc bằng cách tách các nguyên nhân thành các loại chính (được thể hiện bằng đường kẻ nằm ngoài xương sống cá) với các nhánh và nhánh con mô tả nguyên nhân cụ thể hơn của loại đó.



Hình B.5 – Ví dụ về biểu đồ Ishikawa hay biểu đồ xương cá

Sự biểu diễn hình cây tương tự như cây lỗi về hình thức bên ngoài, mặc dù nó thường được hiển thị với việc xây dựng cây từ trái sang phải thay vì từ trên xuống dưới. Tuy nhiên, nó không thể được lượng hóa để đưa ra xác suất của sự kiện đầu vì các nguyên nhân là các yếu tố cấu thành có thể chứ không phải là các sai lỗi với xác suất xảy ra đã biết.



Hình B.6 – Ví dụ về sự hình thành cây trong phân tích nguyên nhân và tác động

Biểu đồ nguyên nhân và tác động thường được sử dụng một cách định tính. Có thể giả định xác suất của vấn đề là 1 và ấn định xác suất cho các nguyên nhân chung và sau đó cho các nguyên nhân phụ, trên cơ sở mức độ tin tưởng về sự phù hợp của chúng. Tuy nhiên, các yếu tố cấu thành thường tương tác và đóng góp vào tác động theo các cách phức tạp làm cho việc lượng hóa không có giá trị.

B.17.5 Đầu ra

Đầu ra từ phân tích nguyên nhân và tác động là một biểu đồ xương cá hoặc biểu đồ hình cây chỉ ra các nguyên nhân có thể có và nguyên nhân có khả năng xảy ra. Sau đó điều này được kiểm tra xác nhận và thử nghiệm thực nghiệm trước khi có thể lập ra các khuyến nghị.

B.17.6 Điểm mạnh và hạn chế

Điểm mạnh bao gồm:

- sự tham gia của các chuyên gia thích hợp làm việc trong môi trường nhóm;
- phân tích được cấu trúc;
- xem xét tất cả các giả thuyết có khả năng xảy ra;
- biểu diễn các kết quả bằng đồ thị sẽ dễ thấy;
- các khu vực được nhận biết tại đó có thể cần thêm dữ liệu;
- có thể được sử dụng để nhận biết các yếu tố cấu thành tác động được mong muốn cũng như không mong muốn.Tập trung tích cực vào một vấn đề có thể khuyến khích quan hệ sở hữu và sự tham gia lớn hơn.

Hạn chế bao gồm:

- nhóm có thể không có chuyên môn cần thiết;
- đây không phải là một quá trình đầy đủ và cần là một phần trong phân tích nguyên nhân gốc rễ để đưa ra khuyến nghị;
- đây là một kỹ thuật hiển thị đối với động não tập thể hơn là kỹ thuật phân tích riêng biệt;
- việc tách các yếu tố nguyên nhân thành các loại chính khi bắt đầu phân tích có nghĩa là sự tương tác giữa các loại này có thể không được xem xét thỏa đáng, ví dụ khi sai lỗi thiết bị do lỗi của con người, hoặc các vấn đề của con người do thiết kế kém gây ra.

B.18 Phân tích các lớp bảo vệ (LOPA)

B.18.1 Tổng quan

LOPA là một phương pháp bán định lượng để ước lượng các rủi ro gắn với một sự kiện hoặc tình huống không mong muốn. Nó phân tích xem có các biện pháp thỏa đáng để kiểm soát hoặc giảm nhẹ rủi ro hay không.

Một cặp nguyên nhân – hệ quả được lựa chọn và các lớp bảo vệ ngăn ngừa nguyên nhân dẫn đến hệ quả không mong muốn được nhận biết. Thứ tự tính toán mức độ được thực hiện để xác định xem việc bảo vệ có đủ để giảm bớt rủi ro xuống mức có thể gánh chịu được.

B.18.2 Sử dụng

LOPA có thể chỉ đơn giản được sử dụng một cách định tính để xem xét các lớp bảo vệ giữa một mối nguy hay sự kiện nguyên nhân và một kết quả. Thông thường, cách tiếp cận bán định lượng sẽ được áp dụng để làm quá trình sàng lọc chặt chẽ hơn, ví dụ theo HAZOP hoặc PHA.

LOPA đưa ra cơ sở cho quy định về các lớp bảo vệ độc lập (IPL) và mức độ toàn vẹn về an toàn (các cấp SIL) đối với các hệ thống cung cấp dụng cụ, như được mô tả trong bộ tiêu chuẩn IEC 61508 và tiêu chuẩn IEC 61511, khi xác định các yêu cầu về cấp toàn vẹn về tính an toàn (SIL) đối với các hệ thống dụng cụ an toàn. LOPA có thể được sử dụng để hỗ trợ việc phân bổ nguồn lực làm giảm thiểu rủi ro một cách hiệu lực bằng cách phân tích việc làm giảm rủi ro được tạo ra bởi mỗi lớp bảo vệ.

B.18.3 Đầu vào

Đầu vào cho với LOPA bao gồm

- thông tin cơ bản về những rủi ro bao gồm các mối nguy, nguyên nhân và hệ quả như đưa ra ở PHA;
- thông tin về các kiểm soát đặt ra hoặc đề xuất;
- tần số của sự kiện nguyên nhân và xác suất sai lỗi của lớp bảo vệ các thước đo hệ quả và về rủi ro có thể gánh chịu;

- tần số nguyên nhân khởi đầu, xác suất sai lỗi lớp bảo vệ, thước đo hệ quả và một sự xác định về rủi ro có thể chấp nhận được;

B.18.4 Quá trình

LOPA được thực hiện bằng cách sử dụng một nhóm chuyên gia áp dụng quy trình sau:

- nhận biết nguyên nhân khởi đầu đối với một kết quả không mong muốn và tìm kiếm dữ liệu về tần suất và hệ quả của chúng;
- lựa chọn một cặp nguyên nhân – kết quả duy nhất;
- lớp bảo vệ ngăn chặn nguyên nhân dẫn đến hệ quả không mong muốn được nhận biết và được phân tích về hiệu lực của chúng;
- nhận biết các lớp bảo vệ độc lập (IPL) (không phải tất cả các lớp bảo vệ đều là các IPL);
- ước lượng xác suất sai lỗi của mỗi IPL;
- tần suất của nguyên nhân khởi đầu được kết hợp với xác suất sai lỗi IPL và xác suất mọi nhân tố bổ sung có điều kiện (nhân tố bổ sung có điều kiện ví dụ là xem một người sẽ có mặt để gánh chịu tác động hay không) để xác định tần số xuất hiện của hệ quả không mong muốn. Thứ tự về mức độ được sử dụng cho tần suất và xác suất.
- các mức rủi ro được tính toán được so sánh với mức gánh chịu rủi ro để xác định xem có cần bảo vệ thêm không.

IPL là một hệ thống thiết bị hoặc hành động có khả năng ngăn ngừa một tình huống dẫn đến hệ quả không mong muốn của nó, sự độc lập của sự kiện nguyên nhân hay bất kỳ lớp bảo vệ nào khác phù hợp với tình huống.

IPL bao gồm:

- tính năng thiết kế;
- thiết bị bảo vệ vật lý;
- các hệ thống khóa xen kẽ và hệ thống đóng;
- thiết bị báo động quan trọng sự can thiệp bằng tay;
- bảo vệ vật lý sau sự kiện;
- các hệ thống ứng phó khẩn cấp (các quy trình và kiểm tra không phải là các IPL).

B.18.5 Đầu ra

Đưa ra khuyến nghị về mọi sự kiểm soát thêm và hiệu lực của những kiểm soát này trong việc làm giảm rủi ro.

LOPA là một trong những kỹ thuật được sử dụng cho việc đánh giá SIL khi xử lý các hệ thống liên

quan đến được trang bị dụng cụ an toàn.

B.18.6 Điểm mạnh và hạn chế

Điểm mạnh bao gồm:

- yêu cầu thời gian và nguồn lực ít hơn phân tích cây lỗi hoặc đánh giá định lượng rủi ro một cách đầy đủ nhưng lại nghiêm ngặt hơn so với các đánh giá định tính chủ quan;
- giúp nhận biết và tập trung nguồn lực vào các lớp bảo vệ quan trọng nhất;
- nhận biết các hoạt động, hệ thống và quá trình trong đó có những biện pháp bảo vệ không đầy đủ;
- tập trung vào những hệ quả nghiêm trọng nhất.

Hạn chế bao gồm:

- LOPA tập trung vào một cặp nguyên nhân – hệ quả và một tình huống tại một thời điểm, không bao quát được tương tác phức tạp giữa các rủi ro hoặc giữa các kiểm soát.
- rủi ro được lượng hóa có thể không tính đến những phương thức sai lỗi phổ biến;
- LOPA không áp dụng đối với tình huống rất phức tạp trong đó có nhiều cặp nguyên nhân – hệ quả hoặc có nhiều hệ quả tác động đến các bên liên quan khác nhau.

B.18.7 Tài liệu tham khảo

IEC 61508 (tất cả các phần), An toàn chức năng của các hệ thống liên quan đến an toàn điện/điện tử/ lập trình điện tử.

IEC 61511, An toàn chức năng – Các hệ thống trang bị an toàn đối với quá trình của ngành công nghiệp.

B.19 Phân tích cây quyết định

B.19.1 Tổng quan

Cây quyết định thể hiện các cho quyết định thay thế nhau và các kết quả một cách tuần tự tính đến các kết quả không chắc chắn. Nó tương tự cây sự kiện trong đó bắt đầu từ một sự kiện khởi đầu hoặc một quyết định ban đầu và mô hình hóa lộ trình và kết quả từ các sự kiện có thể xảy ra và các quyết định khác nhau có thể được đưa ra.

B.19.2 Sử dụng

Cây quyết định được sử dụng trong quản lý rủi ro dự án và trong các trường hợp khác để giúp lựa chọn quá trình hành động tốt nhất nếu có sự không chắc chắn. Thể hiện bằng đồ thị cũng có thể giúp truyền đạt các lý do cho quyết định.

B.19.3 Đầu vào

Kế hoạch dự án với các điểm quyết định. Thông tin về các kết quả có thể có từ quyết định và về những

sự kiện cơ hội có thể ảnh hưởng đến quyết định.

B.19.4 Quá trình

Cây quyết định bắt đầu bằng một quyết định ban đầu, ví dụ để tiến hành dự án A chứ không phải là dự án B. Khi hai dự án giả định được tiến hành, các biến cố khác nhau sẽ xảy ra và các quyết định khác nhau có thể được dự đoán sẽ cần được đưa ra. Những quyết định được thể hiện dưới dạng cây, tương tự như cây sự kiện. Xác suất của các sự kiện có thể được ước lượng cùng với chi phí hay tính hữu dụng của kết quả cuối cùng trong lộ trình.

Thông tin liên quan về lộ trình quyết định tốt nhất là hợp lý trong đó đưa ra giá trị cao nhất được dự kiến được tính toán vì sản phẩm của tất cả các xác suất có điều kiện cùng theo lộ trình và giá trị kết quả.

B.19.5 Đầu ra

Đầu ra bao gồm:

- phân tích hợp lý về rủi ro thể hiện các lựa chọn khác nhau có thể được thực hiện;
- tính toán giá trị dự kiến đối với mỗi lộ trình có thể có.

B.19.6 Điểm mạnh và hạn chế

Điểm mạnh bao gồm:

- đưa ra biểu diễn rõ ràng bằng đồ thị về chi tiết của một vấn đề quyết định;
- cho phép tính toán lộ trình tốt nhất thông qua một tình huống.

Hạn chế bao gồm:

- các cây quyết định lớn có thể trở nên quá phức tạp cho việc trao đổi thông tin một cách dễ dàng với những người khác;
- có thể có xu hướng đơn giản hóa quá mức tình huống để có thể thể hiện nó theo biểu đồ cây.

B.20 Đánh giá độ tin cậy của con người (HRA)

B.20.1 Tổng quát

Đánh giá độ tin cậy của con người (HRA) xử lý tác động của con người tới việc thực hiện hệ thống và có thể được sử dụng để đánh giá những ảnh hưởng do lỗi của con người tới hệ thống.

Nhiều quá trình bao gồm cả sự tiềm ẩn đối với lỗi con người, đặc biệt khi thời gian sẵn có để người vận hành ra quyết định là ngắn. Xác suất các vấn đề sẽ phát triển một cách đầy đủ và trở nên nghiêm trọng có thể là nhỏ. Tuy nhiên, đôi khi hành động của con người sẽ chỉ là bảo vệ ngăn ngừa một sai lỗi khởi đầu không tiến triển thành một tai nạn.

Tầm quan trọng của HRA đã được minh họa bằng các tai nạn khác nhau trong đó các lỗi nghiêm trọng

của con người đóng góp vào một chuỗi các sự kiện tham khảo. Những tai nạn này là các cảnh báo đối với việc đánh giá rủi ro chỉ tập trung vào phần cứng và phần mềm trong một hệ thống. Chúng minh họa cho những nguy hiểm của việc bỏ qua xác suất của sự đóng góp lỗi con người. Hơn nữa, HRA hữu ích trong việc nhấn mạnh các lỗi có thể cản trở đến năng suất và tiết lộ các cách thức theo đó những lỗi này và các sai lỗi khác (phần cứng và phần mềm) có thể được "phục hồi" bằng các yếu tố vận hành của con người và nhân viên bảo trì.

B.20.2 Sử dụng

HRA có thể được sử dụng một cách định tính hoặc định lượng. Một cách định tính, nó được dùng để nhận biết sự tiềm ẩn đối với lỗi con người và nguyên nhân nó vì vậy xác suất của lỗi có thể được giảm. HRA định lượng được dùng để đưa dữ liệu về sai lỗi con người vào FTA hoặc kỹ thuật khác.

B.20.3 Đầu vào

Đầu vào cho HRA bao gồm:

- thông tin để xác định các nhiệm vụ mà con người cần thực hiện;
- kinh nghiệm về các loại lỗi xảy ra trong thực tế hoặc khả năng tiềm ẩn lỗi;
- kiến thức chuyên môn về lỗi của con người và lượng hóa nó.

B.20.4 Quá trình

Quá trình HRA như sau:

- **Xác định vấn đề**, các kiểu liên quan của con người được kiểm tra/đánh giá là gì?
- **Phân tích nhiệm vụ**, nhiệm vụ sẽ được thực hiện ra sao và kiểu hỗ trợ nào sẽ cần để hỗ trợ việc thực hiện?
- **Phân tích lỗi con người**, việc thực hiện nhiệm vụ có thể mắc lỗi như thế nào: những lỗi nào có thể xảy ra và chúng có thể được phục hồi như thế nào?
- **Thể hiện**, những lỗi này hoặc sai lỗi trong việc thực hiện nhiệm vụ có thể được kết hợp ra sao với phần cứng, phần mềm và các sự kiện môi trường khác để cho phép tính toán toàn bộ xác suất sai lỗi toàn bộ hệ thống?
- **Sàng lọc**, có các lỗi hoặc nhiệm vụ không cần xác định số lượng chi tiết hay không?
- **Lượng hóa**, những lỗi và sai lỗi của các nhiệm vụ riêng lẻ có khả năng xảy ra như thế nào?
- **Đánh giá tác động**, những lỗi hoặc nhiệm vụ nào là quan trọng nhất, nghĩa là những lỗi hoặc nhiệm vụ có đóng góp lớn nhất đến độ tin cậy hoặc rủi ro?
- **Làm giảm lỗi**, có thể đạt được độ tin cậy cao hơn của con người như thế nào?
- **Lập tài liệu**, những chi tiết nào của HRA cần được lập thành văn bản?

Trong thực tế, quá trình HRA tiến hành bước hình bậc thang mặc dù đôi khi có các phần (ví dụ phân

tích nhiệm vụ và nhận biết lỗi) tiến hành song song với nhau.

B.20.5 Đầu ra

Đầu ra bao gồm:

- danh mục lỗi có thể xảy ra và các phương pháp có thể giảm lỗi – tốt nhất là thông qua thiết kế lại hệ thống;
- phương thức lỗi, loại lỗi, các nguyên nhân và hệ quả;
- đánh giá định lượng hay định tính rủi ro do lỗi này gây ra.

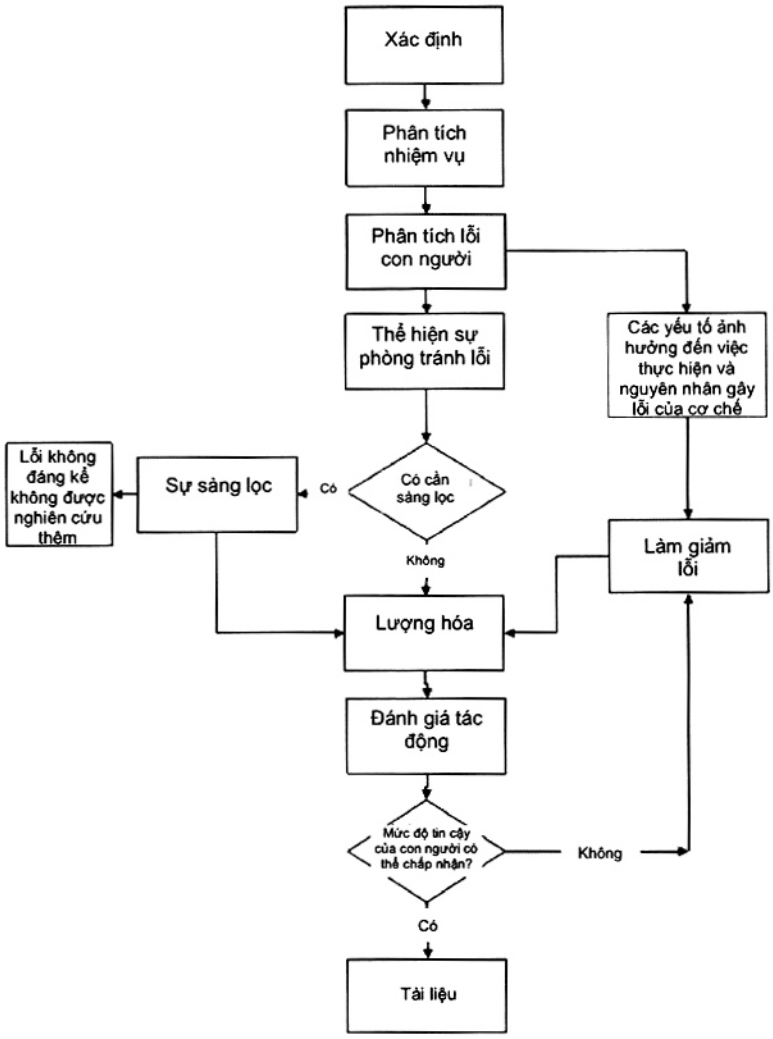
B.20.6 Điểm mạnh và hạn chế

Điểm mạnh của HRA bao gồm:

- HRA đưa ra một cơ chế chính thức để đưa lỗi của con người vào xem xét những rủi ro liên quan đến hệ thống trong đó con người thường đóng vai trò quan trọng;
- xem xét chính thức các phương thức lỗi của con người và các cơ chế có thể giúp làm giảm xác suất của sai lỗi do con người

Hạn chế bao gồm:

- tính phức tạp và biến đổi của con người sẽ làm việc xác định các phương thức và xác suất sai lỗi đơn giản trở nên khó khăn;
- nhiều hoạt động của con người không có một phương thức đơn giản là đạt/không đạt. HRA có khó khăn trong việc xử lý những sai lỗi thành phần hoặc sai lỗi về chất lượng hay việc ra quyết định kém.



Hình B.7 – Ví dụ về đánh giá độ tin cậy của con người

B.21 Phân tích hình nơ bướm

B.21.1 Tổng quát

Phân tích hình nơ bướm là cách lập sơ đồ đơn giản để mô tả và phân tích lộ trình rủi ro từ nguyên nhân đến hệ quả. Nó có thể được coi là sự kết hợp tư duy cây lỗi nguyên nhân của một sự kiện (được thể hiện ở nút thắt của nơ hình bướm) và cây sự kiện phân tích hệ quả. Tuy nhiên, trọng tâm của nơ hình bướm nằm ở những rào cản giữa nguyên nhân và rủi ro, giữa rủi ro và hệ quả. Sơ đồ nơ hình bướm có thể được xây dựng bắt đầu từ cây lỗi và sự kiện, nhưng thường được rút ra trực tiếp từ một cuộc họp động não tập thể hơn.

B.21.2 Sử dụng

Phân tích hình nơ bướm dùng để biểu diễn một rủi ro cho thấy một loạt các nguyên nhân và hệ quả có thể có. Nó được dùng khi tình huống không đảm bảo tính phức tạp của phân tích cây lỗi đầy đủ hoặc khi tập trung nhiều hơn vào việc đảm bảo có một rào cản hoặc sự kiểm soát cho mỗi lộ trình sai lỗi. Nó hữu ích khi có các lộ trình độc lập rõ ràng dẫn đến sai lỗi.

Phân tích hình nơ bướm thường dễ hiểu hơn cây lỗi và sự kiện và do đó có thể là một công cụ trao đổi thông tin hữu ích khi trong đó được việc phân tích bằng cách sử dụng nhiều kỹ thuật phức tạp hơn.

B.21.3 Đầu vào

Đòi hỏi một sự am hiểu thông tin về các nguyên nhân và hệ quả của một rủi ro và các rào cản và kiểm soát có thể ngăn ngừa, giảm nhẹ hoặc thúc đẩy nó.

B.21.4 Quá trình

Nơ hình bướm được vẽ như sau:

a) Một rủi ro cụ thể được nhận diện để phân tích và được thể hiện ở nút thắt trung tâm của nơ.

b) Nguyên nhân của sự kiện được liệt kê bởi việc xem xét các nguồn rủi ro (hoặc mối nguy trong một bối cảnh liên quan đến an toàn).

c) Cơ chế theo đó nguồn rủi ro dẫn đến sự kiện quan trọng được nhận biết;

d) Các đường được vẽ giữa mỗi nguyên nhân và sự kiện hình thành nửa bên trái của nơ. Các yếu tố có thể dẫn đến sự phát triển có thể được nhận biết và đưa vào sơ đồ.

e) Rào cản ngăn ngừa mỗi nguyên nhân dẫn đến hệ quả không mong muốn có thể được biểu diễn bởi các vạch dọc cắt qua đường kẻ. Nếu có các yếu tố có thể gây ra sự phát triển, các rào cản đối với sự phát triển cũng có thể được thể hiện. Cách tiếp cận này cũng có thể dùng cho những hệ quả tích cực trong đó các vạch phản ánh "các kiểm soát" thúc đẩy sự hình thành của sự kiện.

f) Ở phía bên phải của nơ các hệ quả tiềm ẩn khác nhau của rủi ro được nhận biết và các đường được vẽ tỏa ra từ sự kiện rủi ro đến từng hệ quả tiềm ẩn.

g) Các rào cản đối với hệ quả được vẽ bởi các vạch cắt qua đường xuyên tâm. Cách tiếp cận này có thể dùng đối với hệ quả tích cực trong đó các thanh phản ánh "các kiểm soát" hỗ trợ sự hình thành các hệ quả.

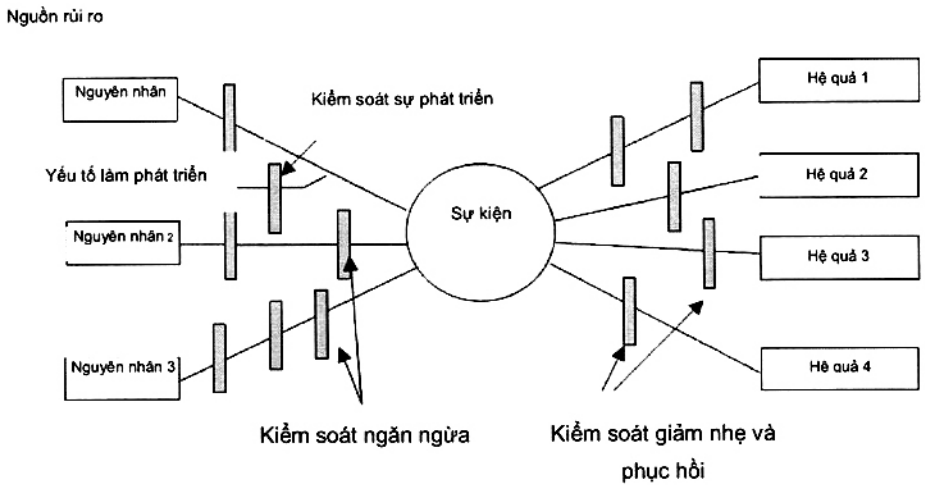
h) Các chức năng quản lý hỗ trợ kiểm soát (như đào tạo và kiểm tra) có thể được biểu diễn theo nơ hình bướm và được liên kết tới kiểm soát tương ứng.

Mức độ định lượng hóa nhất định của sơ đồ hình nơ bướm có thể thực hiện khi các lộ trình là độc lập, xác suất của một hệ quả hay kết quả cụ thể đã biết và có thể ước lượng con số đối với hiệu lực của kiểm soát. Tuy nhiên, trong nhiều tình huống, các lộ trình và các rào cản không độc lập và các kiểm soát có thể mang tính quy trình và do đó hiệu lực không rõ ràng. Việc lượng hóa thường được thực

hiện một cách phù hợp hơn bằng cách sử dụng FTA và ETA.

B.21.5 Đầu ra

Đầu ra là sơ đồ đơn giản thể hiện những lộ trình rủi ro chính và các rào cản đặt ra để ngăn ngừa hoặc giảm nhẹ hệ quả không mong muốn hay thúc đẩy hệ quả mong muốn.



Hình B.8 – Ví dụ sơ đồ hình nơ bướm đối với các hệ quả không mong muốn

B.21.6 Điểm mạnh và hạn chế

Điểm mạnh của phân tích hình nơ bướm:

- đơn giản để hiểu biết và đưa ra một sự hiển thị vấn đề bằng hình ảnh rõ ràng;
- tập trung sự chú ý vào các kiểm soát được đề xuất đặt ra cho cả việc ngăn ngừa và giảm nhẹ và hiệu lực của chúng;
- có thể được sử dụng đối với hệ quả mong muốn;
- không cần sử dụng trình độ chuyên môn cao.

Hạn chế bao gồm:

- không thể mô tả nhiều nguyên nhân xảy ra đồng thời gây ra các hệ quả (nghĩa là khi có các cổng VÀ trong cây lỗi vẽ ra nửa bên trái của nơ);
- có thể quá đơn giản hóa các tình huống phức tạp, cụ thể là cố gắng lượng hóa.

B.22 Bảo trì tập trung vào sự tin cậy

B.22.1 Tổng quan

Bảo trì tập trung vào sự tin cậy (RCM) là một phương pháp nhận biết các chính sách cần phải được thực hiện để quản lý các sai lỗi để đạt được hiệu lực và hiệu quả sự an toàn cần thiết, sự sẵn có và tính kinh tế trong vận hành tất cả các loại thiết bị.

Hiện nay, RCM là phương pháp luận đã được chứng minh và được chấp nhận sử dụng rộng rãi trong nhiều ngành công nghiệp.

RCM đưa ra một quá trình quyết định để nhận biết các yêu cầu bảo trì dự phòng thích hợp và hiệu lực đối với thiết bị phù hợp với các hệ quả về an toàn, vận hành và kinh tế của các sai lỗi được nhận biết và cơ chế suy giảm chất lượng của máy móc chịu trách nhiệm cho những sai lỗi đó. Kết quả làm việc cuối cùng thông qua quá trình là một sự đánh giá sự cần thiết của việc thực hiện nhiệm vụ bảo trì hoặc hành động khác như thay đổi trong vận hành. Chi tiết liên quan đến việc sử dụng và ứng dụng RCM được đưa ra ở IEC 60300-3-11.

B.22.2 Sử dụng

Tất cả các nhiệm vụ đều dựa trên sự an toàn liên quan đến con người và môi trường và các vấn đề vận hành hoặc kinh tế. Tuy nhiên, cần lưu ý rằng tiêu chí được xem xét sẽ phụ thuộc vào tính chất của sản phẩm và ứng dụng của nó. Ví dụ, quá trình sản xuất sẽ cần khả thi về phương diện kinh tế và có thể dễ bị ảnh hưởng đối với các xem xét môi trường chặt chẽ, trong khi một hạng mục của thiết bị bảo vệ cần hoạt động thành công, nhưng có thể tiêu chí an toàn, kinh tế và môi trường ít chính xác hơn. Có thể đạt được lợi ích lớn nhất thông qua định hướng việc phân tích tới những khu vực sai lỗi sẽ có các tác động nghiêm trọng về an toàn, môi trường, kinh tế hay vận hành.

RCM được dùng để đảm bảo rằng việc bảo trì thích hợp và hiệu lực được thực hiện và thường được ứng dụng trong giai đoạn thiết kế và phát triển và sau đó được áp dụng trong quá trình vận hành và bảo trì.

B.22.3 Đầu vào

Ứng dụng thành công RCM cần một sự hiểu biết tốt về thiết bị và cấu trúc, môi trường vận hành và các hệ thống, hệ thống con và các hạng mục liên quan của thiết bị, cùng với các sai lỗi có thể có và hệ quả của những sai lỗi đó.

B.22.4 Quá trình

Các bước cơ bản của một chương trình RCM như sau:

- khởi đầu và hoạch định;
- phân tích sai lỗi tính năng;
- lựa chọn nhiệm vụ;

- thực hiện;
- cải tiến liên tục.

RCM dựa vào rủi ro vì nó tuân theo các bước cơ bản trong đánh giá rủi ro. Loại đánh giá rủi ro là phương thức sai lỗi, phân tích tác động và mức độ nghiêm trọng (FMECA), nhưng đòi hỏi cách tiếp cận cụ thể để phân tích khi được sử dụng trong bối cảnh này.

Nhận diện rủi ro tập trung vào các tình huống trong đó sai lỗi tiềm ẩn có thể bị loại bỏ hoặc làm giảm tần số và/hoặc hệ quả bằng cách thực hiện các nhiệm vụ bảo trì. Nó được thực hiện bằng cách nhận biết các chức năng cần thiết, tiêu chuẩn tính năng và sai lỗi của thiết bị và linh kiện có thể cản trở những chức năng đó.

Phân tích rủi ro bao gồm việc ước lượng tần suất của mỗi sai lỗi khi không thực hiện bảo trì. Hệ quả được thiết lập bằng cách xác định các tác động của sai lỗi. Ma trận rủi ro bao gồm tần suất sai lỗi và hệ quả cho phép thiết lập các loại mức rủi ro.

Sau đó, đánh giá rủi ro được thực hiện bằng việc lựa chọn chính sách quản lý sai lỗi thích hợp đối với mỗi phương thức sai lỗi.

Toàn bộ quá trình RCM được lập thành văn bản đầy đủ phục vụ việc tham khảo và xem xét sau này. Thu thập dữ liệu về sai lỗi và dữ liệu liên quan đến bảo trì cho phép theo dõi các kết quả và việc thực hiện cải tiến.

B.22.5 Đầu ra

RCM đưa ra một định nghĩa về các nhiệm vụ bảo trì như theo dõi điều kiện, khôi phục theo lịch trình, thay thế theo lịch trình, phát hiện sai lỗi hoặc không bảo trì dự phòng. Các hành động khác có thể là kết quả từ việc phân tích bao gồm thiết kế lại, những thay đổi đối với thủ tục vận hành hoặc bảo trì hay đào tạo bổ sung. Sau đó, nhận biết khoảng thời gian và nguồn lực cần thiết cho việc thực hiện nhiệm vụ.

B.22.6 Tài liệu tham khảo

IEC 60300-3-11, Quản lý tính tin cậy – Phần 3-11: Hướng dẫn áp dụng – Bảo trì tập trung vào tính tin cậy.

B.23 Phân tích ẩn (SA) và phân tích mạch ẩn (SCA)

B.23.1 Tổng quan

Phân tích ẩn (SA) là một phương pháp luận để nhận biết các lỗi thiết kế. Một điều kiện ẩn là phần cứng, phần mềm tiềm ẩn hay điều kiện được tích hợp có thể gây ra sự kiện không mong muốn hoặc có thể ngăn chặn một sự kiện mong muốn và không do sai lỗi thành phần gây ra. Những điều kiện này được đặc trưng bằng tính chất ngẫu nhiên và khả năng phát hiện sự phát triển trong thử nghiệm hệ thống chuẩn hóa nghiêm ngặt nhất. Các điều kiện ẩn có thể gây ra hoạt động không phù hợp, mất khả năng sẵn có của hệ thống, sự chậm trễ của chương trình hoặc thậm chí tử vong hay thương tích cho nhân sự.

B.23.2 Sử dụng

Phân tích mạch ẩn (SCA) được xây dựng cuối những năm 1960 cho NASA để kiểm tra xác nhận tính toàn vẹn và khả năng hoạt động của thiết kế của họ. Nó là công cụ hữu ích cho việc khám phá các lộ trình không chủ ý của mạch điện và hỗ trợ trong việc đưa ra các giải pháp để cô lập từng chức năng. Tuy nhiên, như công nghệ mới, các công cụ đối với phân tích ẩn cũng đã có tiến bộ. Phân tích ẩn bao gồm và vượt quá phạm vi của phân tích mạch ẩn. Nó có thể định vị các vấn đề ở cả phần cứng và phần mềm sử dụng công nghệ bất kỳ.

Các công cụ phân tích ẩn có thể tích hợp các phân tích như cây lỗi, phân tích phương thức và tác động sai lỗi (FMEA), ước lượng độ tin cậy, v.v.. vào một phân tích duy nhất tiết kiệm thời gian và chi phí dự án.

B.23.3 Đầu vào

Phân tích ẩn là duy nhất từ quá trình thiết kế trong đó sử dụng các công cụ khác nhau (cây mạng lưới, rừng mạng lưới và dòng mạng lưới hoặc các câu hỏi để giúp chuyên gia phân tích nhận biết các điều kiện ẩn) để tìm hiểu một loại vấn đề cụ thể. Cây và rừng mạng lưới là các nhóm hình học tôpô của hệ thống thực tế. Mỗi cây mạng lưới đại diện cho một chức năng phụ và hiển thị tất cả các đầu vào có thể ảnh hưởng đến đầu ra của chức năng phụ. Rừng được xây dựng bằng cách kết hợp các cây mạng lưới góp phần vào một đầu ra cụ thể của hệ thống. Rừng thích hợp thể hiện một đầu ra của hệ thống theo tất cả các đầu vào liên quan của nó. Những điều này cùng với những nội dung khác, trở thành đầu vào để phân tích.

B.23.4 Quá trình

Các bước cơ bản để thực hiện phân tích ẩn bao gồm:

- chuẩn bị dữ liệu;
- xây dựng cây mạng lưới;
- đánh giá các lộ trình của mạng lưới;
- các khuyến nghị và báo cáo cuối cùng.

B.23.5 Đầu ra

Mạch ẩn là một lộ trình không mong đợi hoặc dòng logic trong một hệ thống, theo các điều kiện nhất định, có thể bắt đầu một chức năng không mong muốn hoặc ngăn cản một chức năng mong muốn. Lộ trình này có thể bao gồm phần cứng, phần mềm, các hành động của người vận hành hoặc sự kết hợp các yếu tố này. Mạch ẩn không phải là kết quả của sai lỗi phần cứng nhưng là các điều kiện tiềm ẩn, tình cờ thiết kế vào hệ thống, được mã hóa thành chương trình phần mềm hoặc được kích hoạt bởi lỗi con người. Có bốn loại mạch ẩn:

a) lộ trình ẩn: lộ trình không mong muốn theo đó các dòng điện, năng lượng, trình tự logic đi theo hướng ngoài dự kiến;

b) thời gian ẩn: các sự kiện xảy ra theo một trình tự không mong muốn hoặc xung đột;

c) các chỉ dẫn ẩn: sự hiển thị mơ hồ hay hiển thị sai về các điều kiện vận hành hệ thống có thể gây ra việc hệ thống hoặc người vận hành thực hiện hành động không mong muốn;

d) nhãn ẩn: ghi nhãn về chức năng của hệ thống không đúng hoặc không chính xác, ví dụ đầu vào của hệ thống, các kiểm soát, kênh hiển thị có thể dẫn đến việc người vận hành áp dụng tác động không chính xác cho hệ thống.

B.23.6 Điểm mạnh và hạn chế

Điểm mạnh bao gồm:

- phân tích ẩn tốt cho việc nhận biết các lỗi thiết kế;
- hoạt động tốt nhất khi được áp dụng cùng với HAZOP;
- rất tốt cho việc xử lý các hệ thống có nhiều trạng thái như thiết bị theo khối hoặc bán khối.

Hạn chế bao gồm:

- quá trình có khác biệt nào đó phụ thuộc vào việc nó được áp dụng đối với mạch điện tử, thiết bị quá trình, thiết bị cơ khí hoặc phần mềm;
- phương pháp phụ thuộc vào việc thiết lập cây mạng lưới chính xác.

B.24 Phân tích Markov

B.24.1 Tổng quan

Phân tích Markov được sử dụng khi trạng thái tương lai của hệ thống chỉ phụ thuộc vào trạng thái hiện tại của. Nó thường được sử dụng để phân tích các hệ thống có thể sửa chữa có thể tồn tại ở nhiều trạng thái và cách sử dụng phân tích khối tin cậy không phù hợp để phân tích đầy đủ hệ thống. Phương pháp này có thể được mở rộng cho hệ thống phức tạp hơn bằng cách áp dụng quá trình Markov có trật tự cao hơn và chỉ bị giới hạn bởi mô hình, phép tính toán học và các giả định.

Quá trình phân tích Markov là kỹ thuật định lượng và có thể rời rạc (bằng cách sử dụng xác suất thay đổi giữa các trạng thái) hoặc liên tục (bằng cách sử dụng tỷ lệ thay đổi qua các trạng thái).

Mặc dù phân tích Markov có thể thực hiện bằng tay, nhưng tính chất kỹ thuật của nó cho phép việc sử dụng các chương trình máy tính, nhiều kỹ thuật phân tích có trên thị trường.

B.24.2 Sử dụng

Kỹ thuật phân tích Markov có thể được sử dụng trong cấu trúc hệ thống khác nhau, có hoặc không có sửa chữa, bao gồm:

- các thành phần độc lập tương đương;
- các thành phần độc lập theo bộ;

- hệ thống chia tải;
- hệ thống chờ, bao gồm trường hợp sai lỗi chuyển đổi có thể xảy ra;
- các hệ thống bị xuống cấp.

Kỹ thuật phân tích Markov cũng có thể được dùng để tính toán khả năng sẵn có, bao gồm việc tính đến các linh kiện để sửa chữa.

B.24.3 Đầu vào

Đầu vào thiết yếu cho phân tích Markov như sau:

- danh mục các trạng thái khác nhau của hệ thống, hệ thống phụ hoặc thành phần [ví dụ vận hành đầy đủ, vận hành một phần (nghĩa là trạng thái xuống cấp), trạng thái hư hỏng, v.v...];
- hiểu biết rõ ràng về quá trình chuyển đổi cần được mô hình hóa. Ví dụ, sai lỗi của lốp xe ô tô cần xem xét trạng thái của bánh xe dự trữ và tần suất kiểm tra.
- tỷ lệ thay đổi từ trạng thái này sang trạng thái khác, thường được thể hiện bằng xác suất thay đổi giữa các trạng thái đối với các sự kiện rời rạc, hoặc tỷ lệ sai lỗi (λ) và/hoặc tỷ lệ sửa chữa (μ) đối với các sự kiện liên tục.

B.24.4 Quá trình

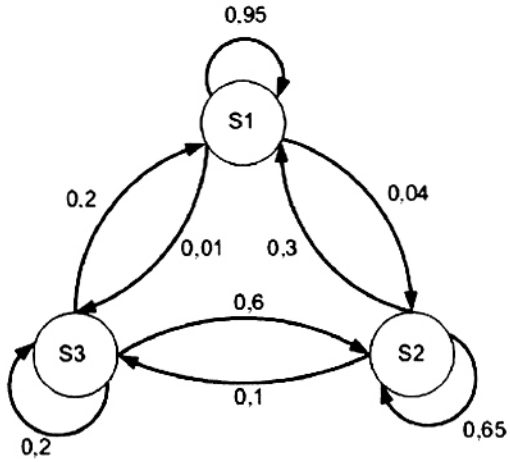
Kỹ thuật phân tích Markov tập trung quanh khái niệm "trạng thái", ví dụ "sẵn có" và "hư hỏng" và sự chuyển đổi giữa hai trạng thái này theo thời gian dựa trên hằng số xác suất thay đổi liên tục. Một ma trận xác suất chuyển đổi ngẫu nhiên được sử dụng để mô tả sự chuyển đổi giữa mỗi trạng thái cho phép việc tính toán các đầu ra khác nhau.

Để minh hoạ cho kỹ thuật phân tích Markov, coi một hệ thống phức tạp chỉ có thể ở ba trạng thái: hoạt động, xuống cấp và hư hỏng, được xác định là trạng thái S1, S2, S3 tương ứng. Mỗi ngày, hệ thống tồn tại ở một trong ba trạng thái này. Bảng B.3 thể hiện xác suất ngày hôm sau, hệ thống ở trạng thái S*i* trong đó *i* có thể là 1,2, hoặc 3.

Bảng B.2 – Ma trận Markov

		Trạng thái hôm nay		
		S1	S2	S3
Trạng thái ngày mai	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

Dãy xác suất này được gọi là ma trận Markov, hoặc ma trận chuyển đổi. Lưu ý rằng tổng của mỗi cột là 1 vì như chúng là tổng của tất cả các kết quả có thể có trong mỗi trường hợp. Hệ thống cũng có thể được thể hiện bằng sơ đồ Markov trong đó các vòng tròn thể hiện trạng thái và các mũi tên thể hiện sự chuyển đổi cùng với xác suất kèm theo.



Hình B.9 – Ví dụ về sơ đồ hệ thống Markov

Các mũi tên chuyển từ một trạng thái tới chính trạng thái đó thường không được thể hiện, nhưng được chỉ ra trong những ví dụ này về sự đầy đủ.

P*i* thể hiện xác suất phát hiện hệ thống ở trạng thái *i*, với *i* = 1,2,3, sau đó giải hệ phương trình:

$$P1 = 0,95\ P1 + 0,30\ P2 + 0,20\ P3 \quad (B.1)$$

$$P2 = 0,04\ P1 + 0,65\ P2 + 0,60\ P3 \quad (B.2)$$

$$P3 = 0,01\ P1 + 0,05\ P2 + 0,20\ P3 \quad (B.3)$$

Ba phương trình này không độc lập và sẽ không tìm ba ẩn số. Phương trình sau cần được sử dụng và một trong những phương trình trên bị loại bỏ.

$$1 = P1 + P2 + P3 \quad (B.4)$$

Đáp số là 0,85; 0,13 và 0,02 đối với các trạng thái tương ứng 1, 2, 3. Hệ thống hoạt động đầy đủ trong 85 % thời gian, ở trạng thái xuống cấp trong 13 % thời gian và ở trạng thái hư hỏng trong 2 % thời gian.

Xem xét hai hạng mục vận hành song song với từng hạng mục cần vạn hành để hệ thống hoạt động. Những hạng mục này có thể vận hành hoặc hư hỏng và khả năng sẵn có của hệ thống phụ thuộc vào trạng thái của những hạng mục đó.

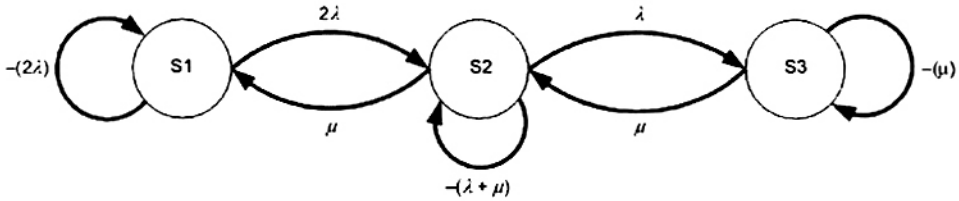
Các trạng thái có thể được coi là:

Trạng thái 1 Cả hai hạng mục hoạt động một cách chính xác

Trạng thái 2 Một hạng mục hỏng và đang tiến hành sửa chữa, hạng mục kia đang hoạt động;

Trạng thái 3 Cả hai hạng mục đều hỏng và một hạng mục đang tiến hành sửa chữa.

Nếu tỷ lệ sai lỗi liên tục đối với mỗi hạng mục được giả định là λ và tỷ lệ sửa chữa là μ, thì sơ đồ chuyển đổi trạng thái là:



Hình B.10 – Ví dụ về sơ đồ chuyển đổi trạng thái

Chú ý rằng sự chuyển đổi từ trạng thái 1 sang trạng thái 2 là 2λ vì sai lỗi của một trong hai hạng mục sẽ chuyển hệ thống sang trạng thái 2.

Đặt P*i*(*t*) là xác suất ở trạng thái ban đầu *i* tại thời điểm *t*; và

Đặt P*i*(*t* + *δt*) là xác suất ở trạng thái cuối cùng tại thời điểm *t* + *δt*

Ma trận xác suất chuyển đổi trở thành:

Bảng B.3 – Ma trận Markov cuối cùng

		Trạng thái ban đầu		
		P1(*t*)	P2(*t*)	P3(*t*)
	P1(*t* + *δt*)	–2λ	*μ*	0
Trạng thái cuối cùng	P2(*t* + *δt*)	2λ	- (*λ* + *μ*)	*μ*
	P3(*t* + *δt*)	0	*λ*	– *μ*

Đáng chú ý là giá trị 0 xảy ra khi không thể chuyển từ trạng thái 1 đến trạng thái 3 hoặc từ trạng thái 3 đến trạng thái 1. Cũng như vậy, tổng các cột bằng không khi quy định tỷ lệ.

Hệ phương trình trở thành:

$dP1/dt = -2\lambda\, P1(t) + \mu\, P2(t)$ (B.5)

$dP2/dt = 2\lambda\, P1(t) + -(\lambda + \mu)\, P2(t) + \mu\, P3(t)$ (B.6)

$dP3/dt = \lambda\, P2(t) + -\mu\, P3(t)$ (B.7)

Để đơn giản, giả định rằng tính sẵn có cần thiết là khả năng sẵn có trạng thái ổn định.

Khi *δt* tiến đến vô cùng, d*Pi*/d*t* sẽ tiến đến không và phương trình sẽ được giải dễ hơn. Phương trình bổ sung được thể hiện trong Phương trình (B.4) ở trên cũng cần được sử dụng.

Bây giờ hương trình hiện tại $A(t) = P1(t) + P2(t)$ có thể được thể hiện là:

$A = P1 + P2$

Do đó $A = (\mu^2 + 2\lambda\mu)/(\mu^2 + 2\lambda\mu + \lambda^2)$

B.24.5 Đầu ra

Đầu ra từ phân tích Markov là các xác suất khác nhau ở các trạng thái khác nhau và do đó là ước lượng về xác suất sai lỗi và/hoặc khả năng sẵn có, một trong những thành phần thiết yếu của một hệ thống.

B.24.6 Điểm mạnh và hạn chế

Điểm mạnh của phân tích Markov bao gồm:

- khả năng tính toán xác suất đối với các hệ thống có khả năng sửa chữa và nhiều trạng thái xuống cấp.

Hạn chế của phân tích Markov bao gồm:

- giả định về hằng số xác suất thay đổi trạng thái; cả sai lỗi hoặc sửa chữa;
- tất cả các sự kiện là độc lập về mặt thống kê vì trạng thái tương lai độc lập với tất cả các trạng thái quá khứ, ngoại trừ đối với trạng thái vào ngày trước đó;
- cần kiến thức về tất cả xác suất thay đổi trạng thái;
- kiến thức về hoạt động ma trận;
- các kết quả là khó truyền đạt với nhân sự không có kỹ thuật.

B.24.7 So sánh

Phân tích Markov tương tự như phân tích Petri-Net bằng cách có thể theo dõi và quan sát trạng thái hệ thống, mặc dù khác với Petri-Net vì Petri Net có thể tồn tại ở nhiều trạng thái tại cùng một thời điểm.

B.24.8 Tài liệu tham khảo

IEC 61078, Kỹ thuật phân tính độ tin cậy – Sơ đồ khối độ tin cậy và các phương pháp *Boolean*

IEC 61165, Áp dụng kỹ thuật *Markov*

ISO/IEC 15909 (tất cả các phần), Kỹ thuật phần mềm và hệ thống – Mạng lưới *Petri* cấp cao

B.25 Mô phỏng Monte Carlo

B.25.1 Tổng quan

Nhiều hệ thống quá phức tạp đối với các tác động của sự không chắc chắn tới hệ thống để mô hình hóa bằng cách sử dụng kỹ thuật phân tích, nhưng chúng có thể được đánh giá bằng cách xem xét các đầu vào theo các biến ngẫu nhiên và thực hiện N phép tính (được gọi là mô phỏng) bằng cách lấy mẫu đầu vào để đạt được N đầu ra có thể có của kết quả mong muốn.

Phương pháp này có thể giải quyết các tình huống phức tạp mà sẽ rất khó để hiểu và giải quyết bằng một phương pháp phân tích. Các hệ thống có thể được xây dựng bằng cách sử dụng bảng tính và các công cụ thông thường khác, nhưng các công cụ tinh tế hơn có thể sẵn có để hỗ trợ các yêu cầu phức

tạp hơn, với chi phí thấp. Đầu tiên khi kỹ thuật này được xây dựng, số lần lặp lại cần thiết cho mô phỏng Monte Carlo làm cho quá trình bị chậm và tốn thời gian, nhưng những tiến bộ về máy tính và phát triển lý thuyết như là lấy mẫu Latin-hypercube, đã làm cho thời gian xử lý hầu như không đáng kể đối với nhiều ứng dụng.

B.25.2 Sử dụng

Mô phỏng Monte Carlo đưa ra một phương thức đánh giá tác động của sự không chắc chắn tới hệ thống trong một loạt các tình huống. Nó thường được sử dụng để đánh giá một loạt các kết quả có thể có và tần số tương đối của giá trị trong phạm vi đó đối với các thước đo định lượng của một hệ thống như chi phí, thời gian, lượng vật liệu, yêu cầu và thước đo tương tự. Mô phỏng Monte Carlo có thể được sử dụng cho hai mục đích khác nhau.

- truyền độ không đảm bảo tới các mô hình phân tích thông thường;
- tính toán xác suất khi kỹ thuật phân tích không thực hiện được.

B.25.3 Đầu vào

Đầu vào cho mô phỏng Monte Carlo là một mô hình hệ thống tốt và thông tin về các loại đầu vào, nguồn không chắc chắn sẽ được thể hiện và đầu ra cần thiết. Dữ liệu đầu vào với độ không đảm bảo được thể hiện bằng các biến ngẫu nhiên với phân bố phân tán ít hơn hay rộng hơn theo mức độ không đảm bảo. Phân bố đều, phân bố tam giác, phân bố chuẩn và phân bố loga chuẩn thường được sử dụng cho mục đích này.

B.25.4 Quá trình

Quá trình như sau:

a) Xác định một mô hình hoặc thuật toán thể hiện sát nhất có thể biểu hiện của hệ thống được nghiên cứu.

b) Mô hình này được chạy nhiều lần bằng cách sử dụng số ngẫu nhiên để tạo ra đầu ra của mô hình (các mô phỏng về hệ thống); Khi ứng dụng để lập mô hình tác động sự không chắc chắn, mô hình ở dạng phương trình đưa ra mối quan hệ giữa các tham số đầu vào và đầu ra. Giá trị được lựa chọn cho đầu vào được lấy từ phân bố xác suất thích hợp thể hiện bản chất của độ không đảm bảo trong những tham số này.

c) Trong cả hai trường hợp máy tính chạy mô hình nhiều lần (thường lên đến 10,000 lần) với các đầu vào khác nhau và đưa ra nhiều kết quả đầu ra. Chúng có thể được xử lý bằng cách sử dụng thống kê thông thường để đưa ra thông tin như giá trị trung bình, độ lệch chuẩn, khoảng tin cậy.

Ví dụ về một mô phỏng được đưa ra dưới đây.

Xem xét trường hợp của hai hạng mục vận hành đồng thời và chỉ một hạng mục cần cho hệ thống hoạt động. Hạng mục đầu tiên có độ tin cậy 0,9 và hạng mục kia có độ tin cậy 0,8.

Có thể xây dựng một bảng tính với các cột như sau.

Bảng B.4 – Ví dụ về mô phỏng Monte Carlo

	Hạng mục 1		Hạng mục 2		
Số mô phỏng	Số ngẫu nhiên	Hoạt động	Số ngẫu nhiên	Hoạt động	Hệ thống
1	0,577 243	CÓ	0,059 355	CÓ	1
2	0,746 909	CÓ	0,311 324	CÓ	1
3	0,541 728	CÓ	0,919 765	KHÔNG	1
4	0,423 274	CÓ	0,643 514	CÓ	1
5	0,917 776	KHÔNG	0,539 349	CÓ	1
6	0,994 043	KHÔNG	0,972 506	KHÔNG	0
7	0,082 574	CÓ	0,950 241	KHÔNG	1
8	0,661 418	CÓ	0,919 868	KHÔNG	1
9	0,213 376	CÓ	0,367 555	CÓ	1
10	0,565 657	CÓ	0,119 215	CÓ	1

Máy phát ngẫu nhiên tạo ra một số giữa 0 và 1 được sử dụng để so sánh với xác suất của mỗi hạng mục để xác định hệ thống có hoạt động hay không. Với 10 lần chạy kết quả 0,9 không nên được hy vọng là một kết quả chính xác. Cách tiếp cận thông thường được xây dựng bằng máy tính để so sánh kết quả tổng như là tiến trình mô phỏng để đạt được mức độ chính xác cần thiết. Trong ví dụ này, kết quả 0,9799 đạt được sau 20.000 phép lặp.

Mô hình trên có thể được mở rộng theo một số cách. Ví dụ:

- mở rộng chính mô hình đó (như xem xét hạng mục thứ hai hoạt động ngay khi hạng mục đầu tiên hỏng);
- thay đổi xác suất cố định cho một biến (một ví dụ điển hình là phân bố tam giác) khi xác suất không thể được xác định chính xác;
- sử dụng tỷ lệ sai lỗi kết hợp với biến ngẫu nhiên để rút ra được thời gian sai lỗi (theo phân bố mũ, Weibull hoặc phân bố thích hợp khác) và xây dựng trong thời gian sửa chữa.

Trong số những điều khác các ứng dụng bao gồm, đánh giá độ không đảm bảo trong dự báo tài chính, hiệu quả đầu tư, chi phí dự án và dự báo lịch trình, các gián đoạn trong quá trình kinh doanh và các yêu cầu bố trí nhân sự.

Kỹ thuật phân tích không thể đưa ra các kết quả phù hợp hoặc khi có độ không đảm bảo trong dữ liệu đầu vào và dẫn đến không đảm bảo trong dữ liệu đầu ra.

B.25.5 Đầu ra

Đầu ra có thể là một giá trị duy nhất, như được xác định trong ví dụ trên, nó có thể là kết quả được thể hiện bằng phân bố xác suất hoặc tần số hoặc nó có thể là sự nhận biết các hàm chính trong mô hình có tác động lớn nhất đến đầu ra.

Nhìn chung, mô phỏng Monte Carlo sẽ được sử dụng để đánh giá hoặc phân bố toàn bộ các kết quả có thể phát sinh hoặc thước đo chính từ phân bố như là:

- xác suất kết quả phát sinh xác định;
- giá trị của một kết quả trong đó người sở hữu vấn đề có sự tin cậy nhất định sẽ không bị vượt quá hoặc bị phá bỏ, chi phí có ít hơn 10 % cơ hội hoặc vượt quá khoảng thời gian nhất định là 80 % bị vượt quá .

Phân tích về mối quan hệ giữa đầu vào và đầu ra có thể làm sáng tỏ tầm quan trọng tương đối của các yếu tố công việc và nhận biết các mục tiêu hữu ích đối với những nỗ lực ảnh hưởng đến độ không đảm bảo trong kết quả.

B.25.6 Điểm mạnh và hạn chế

Điểm mạnh của phân tích Monte Carlo bao gồm:

- về nguyên tắc, phương pháp này có thể phù hợp với mọi phân bố của biến đầu vào, kể cả các phân bố thực nghiệm bắt nguồn từ các quan sát các hệ thống liên quan;
- các mô hình tương đối đơn giản để xây dựng và có thể được mở rộng khi phát sinh nhu cầu;
- mọi ảnh hưởng hay mối quan hệ phát sinh trong thực tế đều có thể được thể hiện, kể cả các tác động tinh tế như là sự phụ thuộc có điều kiện;
- có thể áp dụng phân tích độ nhạy để nhận biết các ảnh hưởng mạnh và yếu;
- các mô hình có thể dễ hiểu vì mối quan hệ giữa đầu vào và đầu ra là rõ ràng;
- các mô hình hành vi hiệu quả như là Petri Nets (IEC 62551) sẵn có về chứng minh rất hiệu quả đối với mục đích mô phỏng Monte Carlo;
- đưa ra một thước đo về độ chính xác của kết quả;
- phần mềm là sẵn có và tương đối rẻ.

Hạn chế như sau:

- tính chính xác của các giải pháp phụ thuộc vào số lượng mô phỏng có thể được thực hiện (hạn chế này đang ngày càng ít quan trọng với tốc độ xử lý tăng lên của máy tính);
- nó dựa vào khả năng thể hiện độ không đảm bảo trong các tham số của phân bố hợp lý;
- các mô hình lớn và phức tạp có thể là thử thách đối với người lập mô hình và tạo ra khó khăn cho các bên liên quan tham gia quá trình này;

- kỹ thuật có thể không thể cân nhắc đầy đủ các sự kiện hệ quả cao/xác suất thấp và do đó không cho phép sở thích rủi ro của tổ chức được phản ánh trong phân tích.

B.25.7 Tài liệu tham khảo

IEC 61649, Phân tích Weibull

IEC 62551, Kỹ thuật phân tích độ tin cậy – Kỹ thuật mạng lưới *Petri*

ISO/IEC Guide 98-3:2008, Độ không đảm bảo đo – Phần 3: Hướng dẫn về độ không đảm bảo đo (GUM:1995)

B.26 Thống kê Bayes và mạng lưới Bayes

B.26.1 Tổng quan

Thống kê Bayes được quy cho Đức cha Thomas Bayes. Giả thiết của nó là bất kỳ thông tin nào đã biết (Prior) có thể được kết hợp với phép đo tiếp theo (Posterios) để thiết lập xác suất tổng thể. Thể hiện chung của định lý Bayes có thể được biểu diễn như sau:

$$P(A|B) = \{P(A)P(B \mid A)\} / \sum_i P(B \mid E_i)P(E_i)$$

Trong đó

xác suất của X được biểu thị bằng $P(X)$;

xác suất của X với điều kiện Y xảy ra được biểu thị là $P(X|Y)$; và

E_i là sự kiện thứ i.

Ở dạng đơn giản nhất của nó, chuyển thành $P(A|B) = \{P(A)P(B|A)\}/P(B)$.

Thống kê Bayes khác với thống kê truyền thống trong đó không giả định rằng tất cả các tham số phân bố là cố định, mà các tham số đó là biến ngẫu nhiên. Xác suất Bayes có thể được hiểu dễ dàng hơn nếu nó được coi là mức độ tin cậy của một người vào một sự kiện nhất định ngược với cổ điển được dựa trên bằng chứng vật chất. Vì cách tiếp cận của Bayes được dựa trên việc diễn giải chủ quan về xác suất, nên nó đưa ra cơ sở cho tư duy quyết định và xây dựng mạng lưới Bayes (hoặc mạng niềm tin, mạng lưới tín ngưỡng hoặc mạng lưới Bayes).

Mạng lưới Bayes sử dụng một mô hình đồ họa để thể hiện tập hợp các biến và các mối quan hệ xác suất của chúng. Mạng lưới bao gồm các nút thể hiện biến ngẫu nhiên và các mũi tên liên kết nút chính tới nút phụ [trong đó một nút chính là biến ảnh hưởng trực tiếp đến biến (phụ) khác].

B.26.2 Sử dụng

Trong những năm gần đây, việc sử dụng học thuyết và mạng lưới Bays đã trở nên phổ biến rộng rãi một phần vì sức hấp dẫn trực quan của chúng và cũng vì sự sẵn có của các công cụ phần mềm máy tính. Mạng lưới Bayes đã được sử dụng trên một loạt các chủ đề: chẩn đoán y học, mô hình hóa hình ảnh, di truyền, nhận dạng giọng nói, kinh tế học, khám phá không gian và các công cụ tìm kiếm mạnh

qua trang tin điện tử được sử dụng hiện nay. Chúng có giá trị trong mọi lĩnh vực khi có yêu cầu tìm ra các biến chưa biết thông qua vận dụng các mối quan hệ và dữ liệu có kết cấu. Mạng lưới Bayes có thể được sử dụng để tìm hiểu các mối quan hệ nhân quả để đưa ra hiểu biết về một dải vấn đề và dự đoán hệ quả của sự can thiệp.

B.26.3 Đầu vào

Đầu vào tương tự như đầu vào cho mô hình Monte Carlo. Đối với mạng lưới Bayes, ví dụ về các bước thực hiện bao gồm:

- xác định các biến hệ thống;
- xác định mối liên kết nhân quả giữa các biến;
- quy định xác suất điều kiện và xác suất biết trước;
- thêm bằng chứng vào mạng lưới;
- thực hiện việc cập nhật hiểu biết;
- rút ra hiểu biết sau đó.

B.26.4 Quá trình

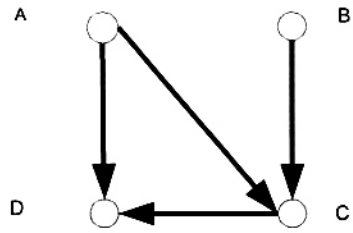
Lý thuyết Bayes có thể được áp dụng theo nhiều cách khác nhau. Ví dụ này sẽ xem xét việc tạo ra một bảng Bayes trong đó xét nghiệm y tế được sử dụng để xác định bệnh nhân có bệnh hay không. Niềm tin trước khi thực hiện xét nghiệm là 99 % dân số không có bệnh này và 1% có bệnh, nghĩa là thông tin đã biết. Độ chính xác của xét nghiệm đã chỉ ra rằng nếu người đó có bệnh, thì kết quả xét nghiệm dương tính 98% theo thời gian. Cũng có khả năng là nếu bạn không có bệnh, thì kết quả xét nghiệm dương tính là 10% theo thời gian. Bảng Bayes đưa ra thông tin như sau:

Bảng B.5 – Dữ liệu bảng Bayes

	THÔNG TIN ĐÃ BIẾT	XÁC SUẤT	SẢN PHẨM	PHÉP ĐO TIẾP THEO
Có bệnh	0,01	0,98	0,009 8	0,090 1
Không có bệnh	0,99	0,10	0,099 0	0,909 9
TỔNG	1		0,108 8	1

Bằng cách sử dụng quy tắc Bayes, sản phẩm được xác định bằng cách kết hợp "Thông tin đã biết" và xác suất. "Phép đo tiếp theo" được thấy bằng cách chia giá trị sản phẩm cho tổng sản phẩm. Đầu ra cho thấy kết quả xét nghiệm dương tính chỉ ra rằng "Thông tin đã biết" đã tăng từ 1% đến 9%. Quan trọng hơn, có một cơ hội lớn là ngay cả với xét nghiệm dương tính việc, có bệnh vẫn không có khả năng xảy ra. Kiểm tra phương trình (0,01×0,98)/[(0,01×0,98)+(0,99×0,1)] cho thấy rằng giá trị 'không có kết quả dương tính với bệnh' đóng vai trò chính trong các giá trị của phép đo tiếp theo.

Xét mạng lưới Bayes sau:



Hình B.11 – Mạng lưới Bayes mẫu

Với xác suất có điều kiện của thông tin đã biết được xác định trong bảng sau và sử dụng các ký hiệu Y chỉ dương tính và N chỉ âm tính, dương tính có thể là "có bệnh" như trên, hoặc có thể là cao và N có thể là thấp.

Bảng B.6 – Xác suất của Thông tin đã biết cho các nút A và B

P(*A* = *Y*)	P(*A* = *N*)	P(*B* = *Y*)	P(*B* = *N*)
0,9	0,1	0,6	0,4

Bảng B.7 – Xác suất có điều kiện đối với nút C với nút A và nút B được xác định

A	*B*	*P(C = Y)*	*P(C = N)*
Y	*Y*	*0,5*	*0,5*
Y	*N*	*0,9*	*0,1*
N	*Y*	*0,2*	*0,8*
N	*N*	*0,7*	*0,3*

Bảng B.8 – Xác suất có điều kiện đối với nút D với nút A và nút C xác định

A	*C*	*P(D = Y)*	*P(D = N)*
Y	*Y*	*0,6*	*0,4*
Y	*N*	*1,0*	*0,0*
N	*Y*	*0,2*	*0,8*
N	*N*	*0,6*	*0,4*

Để xác định xác suất phép đo tiếp theo của P(*A*|*D*=*N*,*C*=*Y*), trước tiên cần tính toán P(*A*,*B*|*D*=*N*,*C*=*Y*).

Bằng cách sử dụng quy tắc Bayes, giá trị P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*) được xác định như chỉ ra dưới đây và cột cuối cùng thể hiện xác suất chuẩn hóa mà tổng là 1 như được suy ra trong ví dụ trước (kết quả được làm tròn).

Bảng B.9 – Xác suất phép đo tiếp theo đối với nút A và B với nút D và nút C xác định

A	*B*	P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*)	P(*A*,*B*|*D*=*N*,*C*=*Y*)
Y	*Y*	0,4 × 0,5 × 0,9 × 0,6 = 0,110	0,4
Y	*N*	0,4 × 0,9 × 0,9 × 0,4 = 0,130	0,48
N	*Y*	0,8 × 0,2 × 0,1 × 0,6 = 0,010	0,04
N	*N*	0,8 × 0,7 × 0,1 × 0,4 = 0,022	0,08

Đưa ra P(*A*|*D*=*N*,*C*=*Y*), cần tính tổng tất cả các giá trị của B:

Bảng B.10 – Xác suất phép đo tiếp theo đối với nút A với nút D và nút C xác định

P(*A*=*Y*|*D*=*N*,*C*=*Y*)	P(*A*=*N*|*D*=*N*,*C*=*Y*)
0,88	0,12

Điều này cho thấy thông tin đã biết khi cho P(*A*=*N*) đã tăng từ 0,1 đến phép đo tiếp theo là 0,12 chỉ là một sự thay đổi nhỏ. Mặt khác, P(*B*=*N*|*D*=*N*,*C*=*Y*) đã thay đổi từ 0,4 đến 0,56 là một sự thay đổi có ý nghĩa hơn.

B.26.5 Đầu ra

Có thể áp dụng cách tiếp cận Bayes ở cùng một mức độ như thống kê cổ điển với một phạm vi rộng đầu ra, ví dụ phân tích dữ liệu để rút ra các ước lượng điểm và khoảng tin cậy. Gần đây tính phổ biến liên quan đến mạng lưới Bayes để đưa ra phân bố cho phép đo tiếp theo. Đầu ra bằng đồ thị đưa ra một mô hình hiểu biết dễ dàng và dữ liệu có thể được sửa đổi dễ dàng để xem xét mối tương quan và độ nhạy của các tham số.

B.26.6 Điểm mạnh và hạn chế

Điểm mạnh:

- tất cả những gì cần thiết là kiến thức về thông tin đã biết;
- tuyên bố suy luận là dễ hiểu;
- các quy tắc Bayes là tất cả những gì cần thiết;
- đưa ra cơ chế cho việc sử dụng kiến thức chủ quan về một vấn đề.

Hạn chế:

- xác định tất cả các tương tác trong mạng lưới Bayes đối với các hệ thống phức tạp là khó giải quyết;
- cách tiếp cận Bayes cần kiến thức về các xác suất có điều kiện thường được đưa ra bởi sự đánh giá của chuyên gia. Các công cụ phần mềm chỉ có thể đưa ra câu trả lời dựa trên những giả định này.

B.27 Đường FN

B.27.1 Tổng quan

Đường FN là sự thể hiện bằng đồ thị xác suất của các sự kiện gây ra một mức nguy hại quy định đối với tổng thể quy định. Chúng thường đề cập nhiều nhất đến tần số của một số thương vong nhất định xảy ra.

Đường FN thể hiện tần số tích lũy (*F*) tại đó *N* hoặc nhiều hơn cá thể của tổng thể sẽ bị ảnh hưởng. Giá trị *N* cao có thể xảy ra với tần số *F* cao, là lợi ích đáng kể vì chúng có thể không thể chấp nhận về mặt xã hội và chính trị.

B.27.2 Sử dụng

Đường cong FN là một cách thể hiện đầu ra của phân tích rủi ro. Nhiều sự kiện có xác suất cao về một kết quả hệ quả thấp và xác suất thấp về một kết quả hệ quả cao. Đường FN đưa ra sự thể hiện về độ rủi ro là một đường mô tả phạm vi này thay vì điểm duy nhất thể hiện một cặp xác suất hệ quả.

Đường FN có thể được sử dụng để so sánh các rủi ro, ví dụ để so sánh những rủi ro được dự đoán theo tiêu chí được xác định bằng đường cong FN, hoặc để so sánh những rủi ro dự đoán với dữ liệu từ những sự cố trong quá khứ, hoặc với tiêu chí quyết định (cũng được được thể hiện bằng đường FN).

Đường FN có thể được sử dụng cho thiết kế hệ thống hay quá trình, hoặc cho việc quản lý các hệ thống hiện tại.

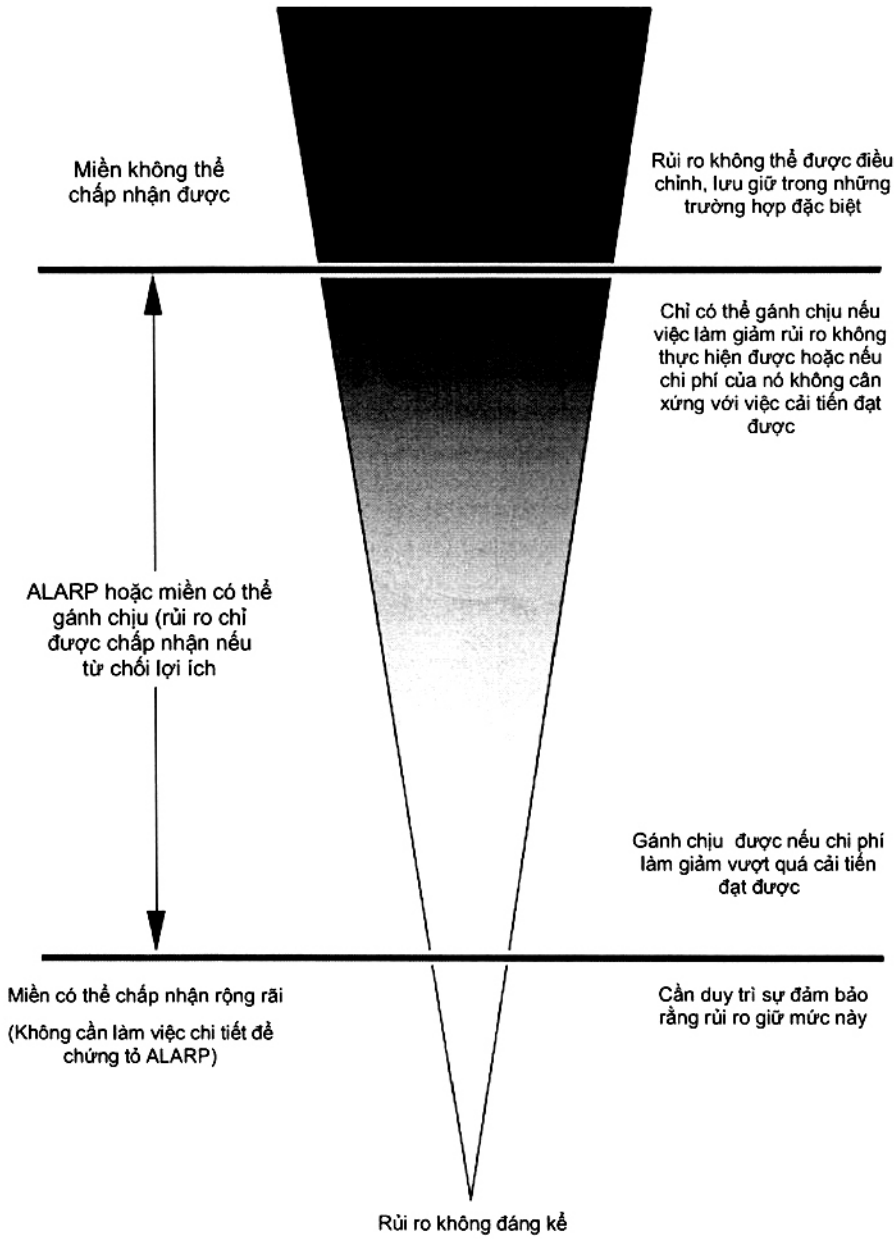
B.27.3 Đầu vào

Các yếu tố đầu vào là:

- các cặp hệ quả xác suất trong một thời gian nhất định;
- đầu ra của dữ liệu từ phân tích định lượng rủi ro bằng cách đưa ra xác suất được ước lượng cho số lượng thương vong quy định;
- dữ liệu từ cả các hồ sơ lịch sử và phân tích định lượng rủi ro.

B.27.4 Quá trình

Dữ liệu sẵn có được vẽ vào một đồ thị với số lượng các thương vong (với một mức nguy hại quy định, nghĩa là chết người tạo thành hoành độ với xác suất N hoặc nhiều thương vong hơn tạo thành tung độ. Do phạm vi lớn các giá trị, cả hai trục thường nằm trên thang logarit.



Hình B.12 – Khái niệm ALARP

Đường FN có thể được xây dựng thống kê bằng cách sử dụng số "thực" từ những mất mát trong quá khứ hoặc chúng có thể được tính toán từ ước lượng mô hình mô phỏng. Dữ liệu được sử dụng và các giả định được lập có thể có nghĩa là hai loại đường FN này đưa ra thông tin khác nhau và cần được sử dụng riêng biệt và cho các mục đích khác nhau. Nhìn chung, đường FN theo lý thuyết là hữu ích nhất cho thiết kế hệ thống và đường FN theo thống kê là hữu ích nhất cho việc quản lý một hệ thống tồn tại cụ thể.

Cả hai cách tiếp cận dẫn xuất có thể tốn thời gian vì vậy nó không phổ biến để sử dụng kết hợp. Sau đó dữ liệu thực nghiệm sẽ hình thành các điểm cố định về những thương vong đã biết một cách chính xác đã xảy ra trong những tai nạn/sự cố đã biết trong khoảng thời gian quy định và phân tích định lượng rủi ro đưa ra các điểm khác bằng ngoại suy hoặc nội suy.

Nhu cầu xem xét những tai nạn có tần số thấp, hệ quả cao có thể đòi hỏi sự xem xét trong khoảng thời gian dài để thu thập đủ dữ liệu cho phân tích thích hợp. Điều này lần lượt làm cho những dữ liệu sẵn có không đáng tin nếu sự kiện đầu xảy ra thay đổi theo thời gian.

B.27.5 Đầu ra

Một đường thể hiện rủi ro cắt qua một loạt các giá trị hệ quả có thể được so sánh với tiêu chí thích hợp đối với tổng thể đang được nghiên cứu và mức độ nguy hại quy định.

B.27.6 Điểm mạnh và hạn chế

Đường FN là cách thể hiện hữu dụng nhất thông tin về rủi ro có thể được người quản lý và những người thiết kế hệ thống sử dụng để giúp đưa ra quyết định về rủi ro và các mức an toàn. Chúng là cách thể hiện hữu ích cả thông tin về tần số và về hệ quả theo một định dạng có thể tiếp cận được.

Đường FN thích hợp cho việc so sánh những rủi ro từ các tình huống tương tự trong đó dữ liệu đầy đủ là sẵn có. Không nên sử dụng chúng để so sánh rủi ro của các loại khác nhau có các đặc trưng khác nhau trong trường hợp số lượng và chất lượng của dữ liệu là biến đổi.

Hạn chế của đường FN là nó không nói lên bất cứ điều gì về một loạt các tác động hoặc kết quả của những sự cố ngoài số lượng người bị ảnh hưởng và không có cách thức nhận biết các cách khác nhau theo đó mức nguy hại xảy ra. Nó chỉ ra một loại hệ quả cụ thể, thường gây tác hại cho con người. Đường FN không phải là một phương pháp đánh giá rủi ro, nhưng là một cách thể hiện các kết quả đánh giá rủi ro.

Đây là một phương pháp thiết lập tốt để thể hiện các kết quả của đánh giá rủi ro nhưng đòi hỏi sự chuẩn bị bởi các nhà phân tích có kỹ năng và thường khó khăn cho những người không phải là chuyên gia để diễn giải và đánh giá.

B.28 Chỉ số rủi ro

B.28.4 Tổng quan

Chỉ số rủi ro là một thước đo rủi ro bán định lượng, là ước lượng thu được bằng cách sử dụng cách cho điểm sử dụng thang đo thứ tự. Chỉ số rủi ro có thể được sử dụng để xếp loại một loạt rủi ro bằng cách dùng các tiêu chí tương tự sao cho chúng có thể được so sánh. Điểm số được áp cho từng thành phần của rủi ro, ví dụ các đặc tính (nguồn) gây ô nhiễm, phạm vi của lộ trình hứng chịu và tác động tới người nhận.

Chỉ số rủi ro là một cách tiếp cận định tính thiết yếu để xếp hạng và so sánh rủi ro. Vì các con số được sử dụng, nên sẽ đơn giản để cho phép thao tác. Trong nhiều trường hợp khi mô hình hoặc hệ thống cơ bản không được biết rõ hoặc không thể thể hiện, sẽ tốt hơn khi sử dụng một cách tiếp cận định tính

rõ ràng hơn.

B.28.2 Sử dụng

Các chỉ số có thể được sử dụng để phân loại những rủi ro khác nhau liên quan đến một hoạt động nếu hệ thống được hiểu rõ. Chúng cho phép sự tích hợp một loạt các yếu tố có ảnh hưởng đến mức rủi ro vào một điểm số duy nhất cho mức rủi ro.

Các chỉ số được sử dụng cho nhiều loại rủi ro khác nhau, thường là một thiết bị xác định phạm vi cho việc phân loại rủi ro theo mức rủi ro. Thiết bị có thể được sử dụng để xác định những rủi ro cần đánh giá sâu hơn có thể và định lượng.

B.28.3 Đầu vào

Đầu vào có nguồn gốc từ phân tích hệ thống, hoặc mô tả bối cảnh. Điều này yêu cầu một sự hiểu biết tốt về các nguồn rủi ro, lộ trình có thể có và những gì có thể bị ảnh hưởng. Các công cụ như phân tích cây lỗi, phân tích cây sự kiện và phân tích quyết định chung có thể được sử dụng để hỗ trợ việc xây dựng chỉ số rủi ro.

Vì việc lựa chọn thang đo thứ tự, ở mức độ nào đó, mang tính tùy tiện, nên cần có đầy đủ dữ liệu để kiểm tra xác nhận chỉ số.

B.28.4 Quá trình

Bước đầu tiên là tìm hiểu và mô tả hệ thống. Khi hệ thống đã được xác định, điểm số được xây dựng cho từng thành phần theo cách mà chúng có thể được kết hợp để đưa ra một chỉ số tổng hợp. Ví dụ, trong bối cảnh môi trường, các nguồn, lộ trình và các nhân tố tiếp nhận sẽ được cho điểm, lưu ý rằng trong một số trường hợp có thể có nhiều lộ trình và nhân tố tiếp nhận đối với mỗi nguồn. Điểm riêng lẻ được kết hợp theo chương trình có tính đến những thực tế vật chất của hệ thống. Quan trọng là điểm số cho từng phần của hệ thống (nguồn, lộ trình và nhân tố tiếp nhận) là phù hợp trong nội bộ và duy trì các mối quan hệ chính xác của chúng. Điểm số có thể được đưa ra cho mỗi thành phần rủi ro (ví dụ xác suất, hứng chịu, hệ quả) hoặc cho các yếu tố làm tăng rủi ro.

Điểm số có thể được cộng, trừ, nhân và/hoặc chia theo mô hình cấp cao này. Tác động tích lũy có thể được tính đến bằng cách cộng điểm (ví dụ cộng vào điểm số đối với các lộ trình khác nhau). Nó tuyệt đối không có ý nghĩa để áp dụng cho công thức toán học với thang đo thứ tự. Do đó, khi xây dựng hệ thống tính điểm, mô hình cần được xác nhận giá trị bằng cách áp dụng với một hệ thống đã biết. Xây dựng một chỉ số là cách tiếp cận lặp lại và một số hệ thống khác nhau để kết hợp điểm số có thể được thử trước khi người phân tích thỏa mãn với việc xác nhận.

Độ không đảm bảo có thể được giải quyết bằng phân tích độ nhạy và thay đổi điểm số để tìm ra các tham số nhạy cảm nhất.

B.28.5 Đầu ra

Đầu ra là một loạt các số (chỉ số tổng hợp) liên quan đến nguồn cụ thể và có thể được so sánh với các chỉ số được xây dựng cho những nguồn khác trong cùng hệ thống hoặc có thể được mô hình hóa theo

cùng một cách.

B.28.6 Điểm mạnh và hạn chế

Điểm mạnh:

- chỉ số có thể đưa ra một công cụ tốt cho việc xếp hạng những rủi ro khác nhau;
- chúng cho phép kết hợp nhiều yếu tố ảnh hưởng đến mức rủi ro vào điểm số duy nhất đối với mức rủi ro.

Hạn chế:

- nếu quá trình (mô hình) và đầu ra của nó không được xác nhận giá trị tốt, thì các kết quả có thể là vô nghĩa. Thực tế đầu ra là giá trị bằng số cho rủi ro có thể bị hiểu sai và sử dụng sai mục đích, ví dụ trong phân tích chi phí/lợi ích tiếp theo.
- trong nhiều tình huống khi sử dụng các chỉ số, không có mô hình cơ bản để xác định xem các thang đo riêng lẻ đối với các yếu tố rủi ro là tuyến tính, logarit hay một dạng thức nào khác hay không và không có mô hình nào xác định cách thức kết hợp các yếu tố. Trong những tình huống này, việc xếp hạng là không đáng tin cậy và xác nhận giá trị theo dữ liệu thực là đặc biệt quan trọng.

B.29 Ma trận hệ quả/xác suất

B.29.1 Tổng quan

Ma trận hệ quả/xác suất là một phương thức kết hợp tỷ lệ hệ quả và xác suất định tính hoặc bán định lượng để đưa ra một mức rủi ro hoặc xếp hạng rủi ro.

Định dạng của ma trận và định nghĩa được áp dụng cho nó phụ thuộc vào bối cảnh sử dụng ma trận và điều quan trọng là thiết kế thích hợp được sử dụng cho những trường hợp này.

B.29.2 Sử dụng

Ma trận hệ quả/xác suất được sử dụng để xếp hạng những rủi ro, nguồn rủi ro hoặc việc xử lý rủi ro trên cơ sở mức rủi ro. Nó thường được sử dụng như một công cụ sàng lọc khi nhiều rủi ro được nhận biết, ví dụ để xác định rủi ro nào cần phân tích thêm hoặc phân tích chi tiết hơn, rủi ro nào cần được xử lý trước hoặc rủi ro nào cần được chuyển tới cấp quản lý cao hơn. Nó cũng được sử dụng để lựa chọn rủi ro nào không cần được xem xét thêm tại thời điểm này. Loại ma trận rủi ro này cũng được sử dụng rộng rãi để xác định một rủi ro nhất định có thể được chấp nhận rộng rãi hoặc không được chấp nhận (xem 5.4) theo vị trí của nó trong ma trận.

Ma trận hệ quả/xác suất cũng có thể được sử dụng để giúp trao đổi sự hiểu biết chung về mức rủi ro định tính trong toàn tổ chức. Cách thức mức rủi ro được thiết lập và các quy tắc quyết định ấn định chúng cần được hài hòa với sở thích rủi ro của tổ chức.

Một hình thức của ma trận hệ quả/xác suất được sử dụng cho phân tích mức độ nghiêm trọng trong FMECA hoặc để thiết lập thứ tự ưu tiên theo HAZOP. Nó cũng được sử dụng trong các tình huống

không có đủ dữ liệu để phân tích chi tiết hoặc tình huống không đảm bảo thời gian và cần phân tích định lượng nhiều hơn.

B.29.3 Đầu vào

Đầu vào cho quá trình là các thang đo được điều chỉnh đối với hệ quả và xác suất và ma trận kết hợp cả hai.

Thang đo hệ quả cần bao trùm một loạt các loại hệ quả khác nhau được xem xét (ví dụ thiệt hại về tài chính; an toàn; môi trường hoặc các thông số khác tùy theo bối cảnh) và cần mở rộng từ hệ quả tin cậy tối đa đến hệ quả quan tâm thấp nhất. Một phần ví dụ được thể hiện trong Hình B.6.

Thang đo có thể có số điểm bất kỳ. Thang điểm 3, 4 hoặc 5 là phổ biến nhất.

Thang đo xác suất cũng có thể có số điểm bất kỳ. Các định nghĩa cho xác suất cần được lựa chọn rõ ràng nhất có thể. Nếu hướng dẫn bằng số được sử dụng để xác định xác suất khác nhau, thì các đơn vị cần được đưa ra. Thang đo xác suất cần mở rộng phạm vi liên quan tới nghiên cứu thực hiện, lưu ý là xác suất thấp nhất phải có thể chấp nhận được đối với hệ quả xác định cao nhất, nếu không tất cả các hoạt động với hệ quả cao nhất được xác định là không thể gánh chịu. Một phần ví dụ được thể hiện trong Hình B.14.

Ma trận được vẽ với hệ quả trên một trục và xác suất trên trục khác. Hình B.15 hiển thị một phần của ma trận ví dụ với thang điểm hệ quả là 6 và thang điểm xác suất là 5.

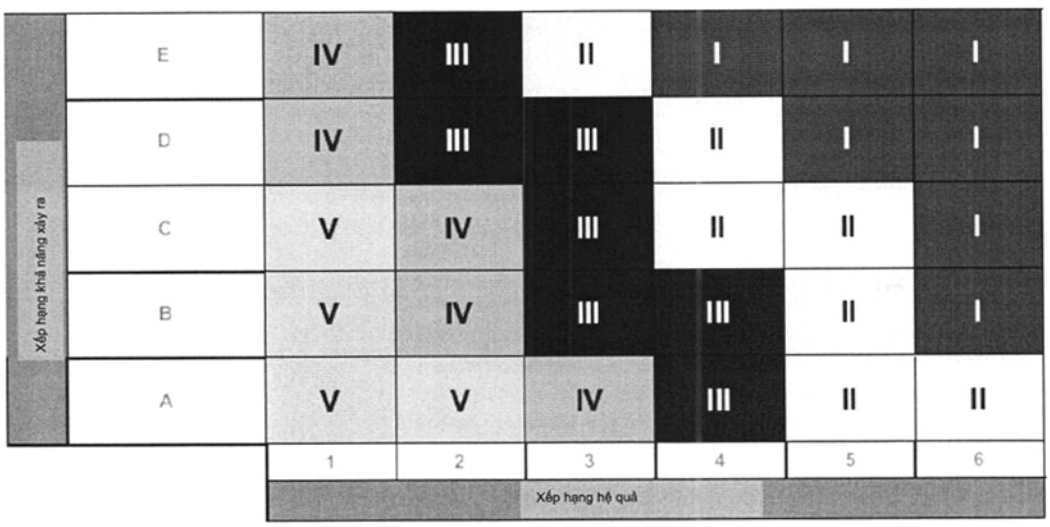
Mức rủi ro được ấn định cho các ô sẽ phụ thuộc vào định nghĩa cho thang hệ quả/xác suất. Ma trận có thể được thiết lập để đưa ra trọng số đặc biệt đối với hệ quả (như được chỉ ra) hoặc xác suất, hoặc nó có thể đối xứng, phụ thuộc vào việc áp dụng. Mức rủi có thể được liên kết với các quy tắc quyết định như là mức độ tập trung quản lý hoặc thang đo thời gian cần đáp ứng.

Rating	Financial Impact AU$ EBITDA	Investment Return AU$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	$100m+ loss or gain	$100 – loss or gain	• Multiple Executive, or • Significant irreversible effects to 10's of people	• Irrecoverable long term environmental harm • Community outrage- potential large-scale class action	• International press reporting over several days • Total loss of shareholder support who act to dismissed. • CEO departs and Board is restructured	• Major litigation or prosecution with damages of $50m+ plus significant costs. • Custodial sentence for company Executive • Prolonged closure of operations by authorities.
5	$10m - $99m loss or gain	$10m - $299m loss or gain	• Single fatality and/or • Severe irreversible disability to one or more persons	• Prolonged environmental impact • High-profile community concerns raised – requiring significant remediation measures.	• National press reporting over several days. • Sustained impact on the reputation of shareholders. • Loss of shareholder support for gro •	• Major litigation costing $10m • Investigation by regulat body resulting in in
4	$1m – $9m loss or gain	$1m – $29m loss or gain	• Extensive injuries or	• Major scr		
3	$100k – $900 loss or gain					
2	$10k					
1						

Hình B.13 – Một phần ví dụ về bảng tiêu chí hệ quả

Rating	Criteria
Likely	- balance of probability will occur, or - could occur within "weeks to months"
Possible	- may occur shortly but a distin - could occur within "mo
Unlikely	- may occur but not - could occur in "
Rare	- occurrence re - exceptional' - only occ
Remote	- theor - fr

Hình B.14 – Một phần ví dụ về ma trận xếp hạng rủi ro



Hình B.15 - Một phần ví dụ về ma trận tiêu chí xác suất

Thang đo tỷ lệ và ma trận có thể được thiết lập với thang đo định lượng. Ví dụ, trong bối cảnh tính tin cậy, thang đo xác suất có thể thể hiện tỷ lệ sai lỗi bằng chỉ số và thang đo hệ quả chi phí bằng tiền của sai lỗi.

Sử dụng công cụ này cần những người (lý tưởng là một nhóm) có chuyên môn phù hợp và dữ liệu như vậy sẵn có để giúp đánh giá hệ quả và xác suất.

B.29.4 Quá trình

Để xếp hạng rủi ro, đầu tiên người sử dụng tìm mô tả hệ quả phù hợp nhất với tình huống, sau đó xác định xác suất với những hệ quả sẽ xảy ra. Tiếp theo, tìm mức rủi ro từ ma trận.

Nhiều sự kiện rủi ro có thể có nhiều kết quả với xác suất liên quan khác nhau. Thông thường, các vấn đề nhỏ phổ biến hơn những tai họa. Do đó có một sự lựa chọn để xếp hạng kết quả phổ biến nhất hoặc nghiêm trọng nhất hoặc sự kết hợp nhất định khác. Trong nhiều trường hợp, thích hợp để tập trung vào kết quả tin cậy nghiêm trọng nhất vì những kết quả này đặt ra đe dọa lớn nhất và thường được quan tâm nhất. Trong một số trường hợp, có thể thích hợp để xếp hạng cả những vấn đề phổ biến và các thảm họa không có khả năng xảy ra như những rủi ro riêng biệt. Quan trọng là xác suất liên quan đến hệ quả được lựa chọn được sử dụng và không phải là xác suất của toàn bộ sự kiện.

Mức rủi ro được xác định bởi ma trận có thể phù hợp với quy tắc quyết định là xử lý hoặc không xử lý rủi ro.

B.29.5 Đầu ra

Đầu ra là một xếp hạng cho mỗi rủi ro hoặc một danh mục rủi ro được xếp hạng với các mức quan trọng được xác định.

B.29.6 Điểm mạnh và hạn chế

Điểm mạnh:

- tương đối dễ để sử dụng;
- đưa ra xếp hạng nhanh chóng rủi ro thành các mức quan trọng khác nhau.

Hạn chế:

- ma trận cần được thiết kế phù hợp với các trường hợp, do đó có thể khó để có một hệ thống chung áp dụng với một loạt các trường hợp liên quan đến một tổ chức;
- khó xác định thang đo một cách rõ ràng;
- việc sử dụng mang tính chủ quan và có xu hướng biến đổi quan trọng giữa các thứ hạng;
- các rủi ro không thể được tổng hợp (nghĩa là một rủi ro không thể xác định rằng số rủi ro thấp cụ thể hoặc một rủi ro thấp được nhận biết số lần cụ thể là tương đương với rủi ro trung bình);
- khó kết hợp hoặc so sánh mức rủi ro đối với các loại hệ quả khác nhau.

Kết quả sẽ phụ thuộc vào mức chi tiết của phân tích, nghĩa là phân tích chi tiết hơn thì số tình huống cao hơn, mỗi phân tích có xác suất thấp hơn. Điều này sẽ ước lượng dưới mức rủi ro thực tế. Cách thức theo đó các tình huống được nhóm lại với nhau trong mô tả rủi ro cần nhất quán và được xác định khi bắt đầu nghiên cứu.

B.30 Phân tích chi phí/lợi ích (CBA)

B.30.1 Tổng quan

Phân tích chi phí/lợi ích có thể được sử dụng để đánh giá rủi ro trong đó tổng chi phí dự kiến có thể đem lại so với tổng lợi ích dự kiến để chọn phương án tốt nhất hoặc lợi nhuận cao nhất. Nó là một phần tiềm ẩn của nhiều hệ thống đánh giá rủi ro. Nó có thể là định tính hay định lượng hoặc đòi hỏi sự kết hợp các yếu tố định lượng và định tính. CBA định lượng cộng dồn giá trị bằng tiền của tất cả chi phí và lợi ích cho tất cả các bên liên quan nằm trong phạm vi sau đó và điều chỉnh theo các khoảng thời gian khác nhau phát sinh chi phí và lợi ích. Giá trị hiện tại ròng (NPV) được đưa ra trở thành đầu vào cho các quyết định về rủi ro. NPV dương liên quan đến một hành động thường có nghĩa là hành động đó nên xảy ra. Tuy nhiên, đối với một số rủi ro tiêu cực, đặc biệt là những rủi ro liên quan đến cuộc sống con người hoặc phá hủy môi trường, có thể áp dụng nguyên tắc ALARP. Nguyên tắc này phân chia rủi ro thành ba vùng: mức trên là các rủi ro tiêu cực không thể gánh chịu và không cần theo đuổi trừ những trường hợp đặc biệt; mức dưới là những rủi ro không đáng kể và chỉ cần theo dõi để đảm bảo chúng duy trì ở mức thấp; và dải ở giữa tại đó rủi ro được làm cho thấp nhất phù hợp với thực tiễn (ALARP). Về phía các rủi ro thấp hơn ở cuối cùng này, phân tích lợi ích chi phí chặt chẽ có thể áp dụng nhưng nếu rủi ro gần như không thể gánh chịu, kỳ vọng của nguyên tắc ALARP là việc xử lý sẽ xảy ra trừ khi chi phí xử lý rất không cân xứng với lợi ích đạt được.

B.30.2 Sử dụng

Phân tích lợi ích/chi phí có thể được dùng để quyết định giữa các phương án liên quan đến rủi ro.

Ví dụ

- làm đầu vào cho quyết định về việc một rủi ro có cần được xử lý hay không;
- để phân biệt và quyết định về hình thức xử lý rủi ro tốt nhất;
- để quyết định giữa các cách thức hành động khác nhau.

B.30.3 Đầu vào

Đầu vào bao gồm thông tin về chi phí và lợi ích cho các bên liên quan thích hợp và về độ không đảm bảo trong chi phí và lợi ích đó. Chi phí và lợi ích hữu hình và vô hình cần được xem xét. Chi phí bao gồm các nguồn lực được mở rộng và các kết quả tiêu cực, lợi ích bao gồm kết quả tích cực, kết quả tiêu cực tránh được và nguồn lực được tiết kiệm.

B.30.4 Quá trình

Các bên liên quan có thể tốn chi phí hoặc nhận được những lợi ích. Trong phân tích chi phí lợi ích đầy đủ của tất cả các bên liên quan sẽ được tính đến.

Nhận biết lợi ích và chi phí trực tiếp và gián tiếp đối với tất cả các bên liên quan thích hợp về các phương án đang được xem xét. Lợi ích trực tiếp là những lợi ích bắt nguồn trực tiếp từ hành động được thực hiện, trong khi lợi ích gián tiếp hoặc phụ thuộc là những lợi ích ngẫu nhiên nhưng có thể

vẫn đóng góp đáng kể vào quyết định. Ví dụ về lợi ích gián tiếp bao gồm nâng cao uy tín, sự thỏa mãn của nhân viên và sự "yên tâm". (Điều này thường có trọng số lớn trong việc ra quyết định).

Chi phí trực tiếp là những chi phí liên quan trực tiếp tới hành động. Chi phí gián tiếp là những chi phí bổ sung, phụ thuộc và chi phí ngầm, như là mất mát tiện ích, sự phân tâm trong thời gian quản lý hoặc chuyển vốn khỏi các đầu tư tiềm ẩn khác. Khi áp dụng phân tích lợi ích chi phí đối với một quyết định về việc có xử lý rủi ro hay không, cần đưa vào chi phí và lợi ích liên quan đến xử lý rủi ro và đến việc theo đuổi rủi ro.

Trong phân tích chi phí/lợi ích định lượng, khi tất cả chi phí và lợi ích hữu hình và vô hình đã được nhận biết, giá trị bằng tiền được ấn định cho tất cả chi phí và lợi ích (kể cả chi phí và lợi ích vô hình). Có một số cách thức chuẩn để thực hiện điều này bao gồm cách tiếp cận 'sẵn sàng chi trả' và sử dụng người thay thế. Nếu, thường xảy ra, chi phí phát sinh qua một khoảng thời gian ngắn (ví dụ một năm) và dòng lợi ích đối với một khoảng thời gian dài sau đó, thì thường cần giảm lợi ích đưa chúng về "giá trị hiện tại" để có thể đạt được một sự so sánh hợp lý. Tất cả chi phí và lợi ích được thể hiện ở giá trị hiện tại. Giá trị hiện tại của tất cả chi phí và lợi ích đối với tất cả các bên liên quan có thể được kết hợp để đưa ra giá trị hiện tại ròng (NPV). NPV dương có nghĩa là hành động có lợi. Tỷ lệ chi phí lợi ích cũng được sử dụng xem B.30.5.

Nếu có sự không đảm bảo về mức chi phí hoặc lợi ích, một hoặc cả hai nội dung này có thể được lấy trọng số theo xác suất của chúng.

Trong phân tích chi phí/lợi ích định tính không có sự nỗ lực nào được đưa ra để thấy một giá trị bằng tiền đối với chi phí và lợi ích vô hình và thay vì đưa ra một con số duy nhất tóm lược chi phí và lợi ích, các mối quan hệ và sự cân bằng giữa chi phí và lợi ích khác nhau được coi là định tính.

Kỹ thuật liên quan là phân tích hiệu quả chi phí. Điều này giả định rằng lợi ích hay kết quả nhất định được mong muốn và có một số cách khác nhau để đạt được nó. Phân tích chỉ tìm kiếm chi phí và cách nào rẻ nhất để đạt được lợi ích.

B.30.5 Đầu ra

Đầu ra của phân tích chi phí/lợi ích là thông tin về chi phí và lợi ích tương đối của các phương án hoặc hành động khác nhau. Điều này có thể được thể hiện một cách định lượng như giá trị hiện tại ròng (NPV), tỉ lệ hoàn vốn nội bộ (IRR), hoặc tỷ lệ giá trị hiện tại của lợi ích với giá trị hiện tại của chi phí. Một cách định tính đầu ra thường là một bảng so sánh chi phí và lợi ích của các loại chi phí và lợi ích khác nhau, tập trung chú ý vào sự cân bằng.

B.30.6 Điểm mạnh và hạn chế

Điểm mạnh của phân tích chi phí lợi ích:

- cho phép chi phí và lợi ích được so sánh bằng cách sử dụng một thước đo duy nhất (bằng tiền);
- đưa ra tính minh bạch của việc ra quyết định;

- nó yêu cầu thông tin chi tiết được thu thập về tất cả các khía cạnh có thể có của quyết định. Điều này có thể có giá trị trong việc bộc lộ sự thiếu hiểu biết cũng như trao đổi thông tin về kiến thức.

Hạn chế:

- CBA định lượng có thể mang lại các con số khác nhau đáng kể, phụ thuộc vào các phương pháp được sử dụng để ấn định giá trị kinh tế cho các lợi ích phi kinh tế.
- trong một số ứng dụng, khó xác định tỷ lệ chiết khấu hợp lý đối với chi phí và lợi ích tương lai;
- lợi ích tích lũy cho một tổng thể lớn là khó ước lượng, những lợi ích cụ thể đó liên quan đến hàng hóa công cộng mà không được trao đổi trên thị trường;
- thực tiễn của phương pháp chiết khấu mà lợi ích đạt được trong tương lai dài hạn có ảnh hưởng không đáng kể đến quyết định phụ thuộc vào tỷ lệ chiết khấu được lựa chọn. Phương pháp trở thành không phù hợp đối với việc xem xét các rủi ro ảnh hưởng đến các thế hệ tương lai trừ phi tỷ lệ chiết khấu được thiết lập rất thấp hoặc bằng không.

B.31 Phân tích quyết định đa tiêu chí (MCDA)

B.31.1 Tổng quan

Mục tiêu là sử dụng một loạt tiêu chí để đánh giá khách quan và minh bạch sự thích hợp tổng thể của một tập hợp các phương án. Nhìn chung, mục đích tổng thể là để đưa ra thứ tự ưu tiên giữa các phương án sẵn có. Việc phân tích đòi hỏi xây dựng một ma trận các phương án và tiêu chí được xếp hạng và được tổng hợp để đưa ra điểm số tổng thể cho từng phương án.

B.31.2 Sử dụng

MCDA có thể được sử dụng để

- so sánh nhiều phương án đối với phân tích vượt qua đầu tiên để xác định các phương án tiềm ẩn, được ưu tiên và phương án không thích hợp,
- so sánh các phương án khi có nhiều tiêu chí và đôi khi có tiêu chí xung đột,
- đạt được sự đồng thuận về một quyết định khi các bên liên quan khác nhau có các mục tiêu hoặc giá trị xung đột.

B.31.3 Đầu vào

Tập hợp các phương án để phân tích. Tiêu chí dựa vào các mục tiêu có thể được sử dụng như nhau thông qua tất cả các phương án để phân biệt chúng.

B.31.4 Quá trình

Nhìn chung một nhóm các bên liên quan có hiểu biết thực hiện quá trình như sau:

a) xác định (các) mục tiêu;

b) xác định các thuộc tính (tiêu chí hoặc thước đo hiệu quả) liên quan đến mỗi mục tiêu;

c) kết cấu các thuộc tính vào một hệ thống phân cấp;

d) xây dựng các phương án được đánh giá theo tiêu chí;

e) xác định tầm quan trọng của tiêu chí và ấn định trọng số tương ứng cho chúng;

f) đánh giá các phương án thay thế theo tiêu chí. Điều này có thể được thể hiện bằng ma trận điểm số;

g) kết hợp nhiều điểm số thuộc tính đơn vào một điểm số duy nhất tổng hợp nhiều thuộc tính;

h) đánh giá kết quả.

Có các phương pháp khác nhau trong đó việc lấy trọng số đối với từng tiêu chí có thể được đưa ra và cách thức khác nhau tổng hợp điểm số tiêu chí đối với mỗi phương án thành điểm số duy nhất nhiều thuộc tính. Ví dụ, các điểm số có thể được tổng hợp lại thành tổng trọng số hoặc sản phẩm có trọng số hoặc bằng cách sử dụng quá trình hệ thống phân tích phân cấp, kỹ thuật suy luận các trọng số và điểm số được dựa trên sự so sánh cặp. Tất cả các phương pháp này giả định rằng sự ưu tiên đối với bất kỳ tiêu chí nào không phụ thuộc vào giá trị của tiêu chí khác. Khi giả định này không có giá trị, mô hình khác được sử dụng.

Vì điểm số mang tính chủ quan, phân tích độ nhạy là hữu ích để kiểm tra bối cảnh tại đó trọng số và điểm số ảnh hưởng đến toàn bộ sự ưu tiên giữa các phương án.

B.31.5 Đầu ra

Thể hiện thứ tự xếp hạng của các phương án từ ưu tiên nhất đến ưu tiên ít nhất. Nếu quá trình đưa ra một ma trận trong đó các trục của ma trận là tiêu chí có trọng số và điểm số của tiêu chí cho từng phương án, thì phương án không có tiêu chí có trọng số cao cũng có thể bị loại bỏ.

B.31.6 Điểm mạnh và hạn chế

Điểm mạnh:

- đưa ra một cấu trúc đơn giản đối với việc ra quyết định hiệu quả và thể hiện các giả định và kết luận;
- có thể đưa ra các vấn đề quyết định phức tạp mà không tuân theo phân tích chi phí/lợi ích, dễ quản lý hơn;
- có thể giúp xem xét các vấn đề một cách hợp lý khi sự cân bằng cần được thiết lập;
- có thể giúp đạt được sự thống nhất khi các bên liên quan có các mục tiêu khác nhau và vì vậy có tiêu chí khác nhau.

Hạn chế:

- có thể bị ảnh hưởng bởi sự thiên lệch và lựa chọn tiêu chí quyết định kém;
- hầu hết các vấn đề của MCDA không có giải pháp kết luận sự ưu tiên duy nhất;
- thuật toán tổng hợp tính toán trọng số của tiêu chí từ các chuẩn được tuyên bố hoặc tổng hợp các quan điểm khác nhau có thể che khuất cơ sở đúng đắn của quyết định.

Thư mục tài liệu tham khảo

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector* (An toàn chức năng – Các hệ thống trang bị an toàn đối với ngành công nghiệp quá trình)

IEC 61508, (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems* (An toàn chức năng của các hệ thống liên quan đến an toàn điện/điện tử/điện tử được lập trình)

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide* (Nghiên cứu và mối nguy và khả năng vận hành (nghiên cứu HAZOP) – Hướng dẫn áp dụng)

TCVN ISO 22000:2007, *Hệ thống quản lý an toàn thực phẩm – Yêu cầu đối với tổ chức trong chuỗi thực phẩm*

TCVN 6844 (ISO/IEC Guide 51) *Hướng dẫn đưa các khía cạnh an toàn vào tiêu chuẩn*

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance* (Quản lý tính tin cậy – Phần 3-11: Hướng dẫn áp dụng – Bảo trì tập trung vào sự tin cậy)

IEC 61649, *Weibull analysis* (Phân tích Weibull)

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods* (Kỹ thuật phân tích tính tin cậy – Sơ đồ khối độ tin cậy và các phương pháp Boolean)

IEC 61165, *Application of Markov techniques* (Áp dụng kỹ thuật Markov)

ISO/IEC 15909, (all parts), *Software and systems engineering – High-level Petri nets* (Kỹ thuật phần mềm và hệ thống – Mạng lưới Petri cấp cao)

IEC 62551, *Analysis techniques for dependability – Petri net techniques* (Kỹ thuật phân tích tính tin cậy – Kỹ thuật mạng Petri)