Mục lục

Lời nói đầu

TCVN 10935-1 : 2015 do Cục Đăng kiểm Việt Nam biên soạn, Bộ Giao thông vận tải đề nghị, Tổng cục Tiêu chuẩn – Đo lường – Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

TCVN 10935-1 : 2015 hoàn toàn tương đương với tiêu chuẩn châu Âu EN 50126-1:1999.

Ứng dụng đường sắt – Quy định và chứng minh độ tin cậy, tính sẵn sàng, khả năng bảo dưỡng và độ an toàn (RAMS) – Phần 1: Các yêu cầu cơ bản và quy trình chung

Railway applications – The specification and demonstration of Reliability, availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process.

1 Phạm vi áp dụng

1.1 Tiêu chuẩn này:

- Quy định RAMS gồm độ tin cậy, tính sẵn sàng, khả năng bảo dưỡng, độ an toàn và sự tương tác giữa các yếu tố này;

- Quy định quy trình quản lý RAMS, dựa trên vòng đời hệ thống và các nhiệm vụ trong vòng đời hệ thống đó;

- Kiểm soát và quản lý có hiệu quả các xung đột có thể xuất hiện giữa các yếu tố RAMS;

- Quy định quy trình có tính hệ thống nhằm xác định rõ các yêu cầu đối với RAMS và quy trình chứng minh việc thỏa mãn những yêu cầu này.

- Đề cập đến các vấn đề cụ thể trong ngành đường sắt.

- Không quy định các chỉ tiêu, số lượng, các yêu cầu hoặc các giải pháp của RAMS đối với các loại hình đường sắt cụ thể.

- Không quy định các yêu cầu đối với việc đảm bảo an ninh hệ thống.

- Không quy định các nguyên tắc hoặc các quy trình có liên quan tới việc chứng nhận các sản phẩm đường sắt theo các yêu cầu của tiêu chuẩn này;

- Không quy định quy trình chứng nhận của cơ quan quản lý nhà nước về an toàn.

1.2 Tiêu chuẩn này áp dụng cho:

- Việc quy định và thuyết minh về RAMS đối với tất cả các loại hình đường sắt ở tất cả các mức độ, từ các tuyến đường sắt hoàn chỉnh cho đến các hệ thống quan trọng trong một tuyến đường sắt, đến các hệ thống con riêng biệt, kết hợp và các tổng thành trong những hệ thống quan trọng, bao gồm cả những hệ thống có phần mềm; đặc biệt đối với:

- Hệ thống mới;

- Hệ thống mới tích hợp vào các hệ thống hiện có đã được đưa vào hoạt động trước khi công bố tiêu chuẩn này nhưng không áp dụng chung cho các hạng mục khác của hệ thống hiện có;

- Đối với việc thay đổi, cải tạo các hệ thống hiện có đã được đưa vào hoạt động trước khi công bố tiêu chuẩn này nhưng không áp dụng chung cho các hạng mục khác của hệ thống hiện có;

- Tại tất cả các giai đoạn liên quan trong vòng đời hệ thống khai thác hoạt động của hệ thống;

- Các doanh nghiệp đường sắt và đơn vị công nghiệp phụ trợ đường sắt khi áp dụng.

CHÚ THÍCH: Hướng dẫn áp dụng được đưa ra trong các yêu cầu của tiêu chuẩn này.

2 Tài liệu viện dẫn

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

EN ISO 9001: 1994, Quality systems – Model for quality assurance in design, development, production, installation and servicing *(Hệ thống chất lượng – Mô hình cho việc đảm bảo chất lượng về thiết kế, xây dựng, sản xuất, lắp đặt và khai thác)*

EN ISO 9002: 1994, Quality systems - Model for quality assurance in production, installation and servicing *(Hệ thống chất lượng – Mô hình cho việc đảm bảo chất lượng về sản xuất, lắp đặt và khai thác)*

EN ISO 9003: 1994, Quality systems – Model for quality assuranca in final inspection and test *(Hệ thống chất lượng – Mô hình cho việc đảm bảo chất lượng khi kiểm tra và thử nghiệm cuối cùng)*

EN 50128, Railway applications – Software for railway control and protection systems *(Hệ thống đường sắt – phần mềm cho các hệ thống kiểm soát và bảo vệ đường sắt)*

EN 50129, Railway applications – Safety related electronic systems for signalling *(Hệ thống đường sắt – Các hệ thống tín hiệu điện tử liên quan tới an toàn)*

IEC 60050, International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service (*Từ vựng kĩ thuật điện quốc tế - Chương 191: Độ tin cậy và chất lượng dịch vụ*)

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

3 Thuật ngữ và định nghĩa

Trong tiêu chuẩn này, có các thuật ngữ và định nghĩa sau:

3.1 Sự phân chia (Apportionment)

Là quá trình chia nhỏ các yếu tố RAMS của một hệ thống thành các hạng mục cấu thành khác nhau để đưa ra các chỉ tiêu riêng biệt.

3.2 Sự đánh giá (Assessment)

Sự tiến hành điều tra để đi đến một kết luận dựa trên bằng chứng về sự phù hợp của một sản phẩm.

3.3 Kiểm toán (Audit)

Là quá trình kiểm tra độc lập có tính hệ thống để xác minh các quy trình lập ra riêng cho các yêu cầu của một sản phẩm có tuân theo các kế hoạch đã định, có được thực hiện một cách hiệu quả và có phù hợp để đạt được các mục tiêu đã định hay không.

3.4 Tính sẵn sàng (Availability)

Khả năng của một sản phẩm ở trong trạng thái thực hiện chức năng được yêu cầu dưới các điều kiện cho trước tại một thời điểm bất kì hoặc trong một khoảng thời gian định trước với giả thiết rằng các nguồn lực bên ngoài theo yêu cầu được đáp ứng.

3.5 Thử hoạt động (Commissioning)

Thuật ngữ chung cho các hoạt động được tiến hành để chuẩn bị cho một hệ thống hoặc sản phẩm trước khi chứng minh nó đáp ứng các yêu cầu cụ thể.

3.6 Hư hỏng có nguyên nhân chung (Common cause failure)

Một hư hỏng là kết quả của (các) sự kiện gây ra sự trùng lặp các tình trạng hư hỏng của hai hoặc nhiều tổng thành dẫn đến hệ thống hư hỏng trong việc thể hiện chức năng được yêu cầu của nó.

3.7 Sự phù hợp (Compliance)

Sự thể hiện một đặc tính hoặc tính năng của một sản phẩm thoả mãn các yêu cầu đã được đặt ra.

3.8 Quản lý cấu hình (Configuration management)

Nguyên tắc áp dụng các biện pháp kĩ thuật, quản lý và giám sát để xác định và lập hồ sơ các đặc điểm về vật lý, chức năng của một thành phần cấu hình, kiểm soát sự thay đổi những đặc điểm này, ghi lại, báo cáo các quá trình thay đổi và tình trạng thực hiện và thẩm tra sự phù hợp với các yêu cầu được quy định.

3.9 Bảo dưỡng sửa chữa (Corrective maintenance)

Hoạt động bảo dưỡng được thực hiện sau khi xác định lỗi và đưa sản phẩm về tình trạng có thể thực hiện được chức năng được yêu cầu.

3.10 Hư hỏng phụ thuộc (Dependent failure)

Hư hỏng do một chuỗi các sự kiện, mà xác suất hư hỏng không thể tínhđược bằng tích đơn giản các xác suất hư hỏng không điều kiện do các sự kiện riêng rẽ gây ra.

3.11 Thời gian dừng (Down time)

Khoảng thời gian mà ở đó sản phẩm ở trạng thái không làm việc (IEC 60050(191)).

3.12 Nguyên nhân hư hỏng (Failure cause)

Các tình huống xảy ra trong quá trình thiết kế, sản xuất hoặc sử dụng có thể dẫn đến hư hỏng (IEC 60050(191)).

3.13 Dạng hư hỏng (Failure mode)

Các kết quả đã được dự đoán hoặc phát hiện trước của một hư hỏng gây ra ở một hạng mục có liên quan tới các điều kiện vận hành tại thời điểm hư hỏng.

3.14 Tỷ lệ hư hỏng (Failure rate)

Nếu tồn tại, là giới hạn của tỉ số của xác suất có điều kiện để thời điểm xảy ra một hư hỏng của sản phẩm ở trong khoảng thời gian cho trước (t, t+Δt) và số gia thời gian Δt khi Δt tiến tới 0, cho rằng hạng mục ở trong trạng thái làm việc tại thời điểm bắt đầu khoảng thời gian.

3.15 Dạng sự cố (Fault mode)

Một trong các tình trạng của sản phẩm có thể bị sự cố về một chức năng được yêu cầu cho trước.

3.16 Phân tích sự cố hình cây (Fault tree analysis)

Phân tích để xác định các dạng sự cố của sản phẩm, sản phẩm phụ hoặc các tình huống bên ngoài, hoặc các kết hợp của chúng, có thể dẫn đến dạng sự cố đã được đưa ra của sản phẩm, thể hiện bằng sự cố dạng cây.

3.17 Nguy hiểm (Hazard)

Trạng thái vật lý có tiềm ẩn gây thương tích về người.

3.18 Sổ tay nguy hiểm (Hazard log)

Tài liệu ghi lại hoặc tham chiếu tất các hoạt động quản lý về an toàn, các rủi ro đã được xác định, các quyết định đã được đưa ra và giải pháp đã được thực hiện, hay còn gọi là "Sổ tay an toàn - *Safety Log*" (theo EN 50129).

3.19 Cung ứng nguồn lực (Logistic support)

Toàn bộ các nguồn lực được sắp xếp và tổ chức để vận hành và duy trì hệ thống đạt được một mức độ khả dụng theo quy định với chi phí vòng đời hệ thống phù hợp.

3.20 Khả năng bảo dưỡng (Maintainability)

Xác suất của một hoạt động bảo dưỡng chủ động theo kế hoạch được thực hiện trong một khoảng thời gian đã định dưới các điều kiện được quy định và sử dụng các quy trình và các nguồn lực cho trước đối với một hạng mục ở điều kiện sử dụng đề ra. (IEC 60050(191)).

3.21 Bảo dưỡng (Maintenance)

Sự kết hợp của các hoạt động kĩ thuật và quản lý, bao gồm các hoạt động giám sát, được dự định để đưa sản phẩm, hoặc khôi phục nó về trạng thái có thể thực hiện được chức năng được yêu cầu (IEC 60050(191)).

3.22 Chính sách bảo dưỡng (Maintenance policy)

Tài liệu mô tả mối tương quan giữa các cấp bảo dưỡng, mức độ ràng buộc và mức độ bảo dưỡng được áp dụng cho việc bảo dưỡng một hạng mục (IEC 60050(191)).

3.23 Nhiệm vụ (Mission)

Sự mô tả có tính mục tiêu của một công việc cơ bản được thực hiện bởi một hệ thống.

3.24 Hồ sơ nhiệm vụ (Mission profile)

Tài liệu tóm tắt các giai đoạn và sự thay đổi dự tính trong nhiệm vụ đối với các thông số như thời gian, khối lượng, tốc độ, khoảng cách, điểm dừng, hầm… trong các giai đoạn vận hành của vòng đời hệ thống.

3.25 Bảo dưỡng phòng ngừa (Preventive maintenance)

Việc bảo dưỡng được thực hiện tại một khoảng thời gian được xác định trước hoặc theo các chỉ tiêu định mức và nhằm giảm xác suất hư hỏng hoặc suy giảm chức năng của một hạng mục (IEC 60050(191)).

3.26 Doanh nghiệp đường sắt (Railway Authority)

Tổ chức có quyền điều hành để vận hành hệ thống đường sắt

CHÚ Ý: Trách nhiệm kiểm soát của doanh nghiệp đường sắt đối với toàn bộ hệ thống hoặc từng phần hệ thống và các hoạt động mang tính chu trình đôi khi sẽ bị phân chia giữa một hoặc nhiều tổ chức hoặc pháp nhân. Ví dụ:

- Đơn vị sở hữu một hoặc nhiều tổng thành trong cơ sở vật chất hệ thống và các đối tác mua hàng của họ;
- Đơn vị vận hành hệ thống;
- Đơn vị bảo dưỡng một hoặc nhiều bộ phận của hệ thống;
- …

Việc phân chia này sẽ dự trên các quy định pháp luật hoặc các thỏa thuận hợp đồng. Những trách nhiệm này nên được tuyên bố rõ ràng ở các giai đoạn đầu của vòng đời hệ thống.

3.27 Đơn vị công nghiệp phụ trợ đường sắt (Railway support industry)

Cụm từ chung nói về các nhà cung ứng cho các hệ thống đường sắt, các hệ thống con hoặc các tổng thành hệ thống hoàn chỉnh.

3.28 Chương trình RAM (RAM programme)

Là một chương trình ghi lại các hoạt động, các nguồn lực và các sự kiện theo kế hoạch để thực hiện các cơ cấu tổ chức, các trách nhiệm, các quy trình, các hoạt động, các khả năng và các nguồn lực kết hợp với nhau để đảm bảo một hạng mục sẽ thỏa mãn các yêu cầu RAM cho trước liên quan tới hợp đồng hoặc dự án đã biết (IEC 60050(191)).

3.29 RAMS

Một cụm từ viết tắt kết hợp từ Độ tin cậy (Reliability), Tính sẵn sàng (Availability), Khả năng bảo dưỡng (Maintainability) và Độ an toàn (Safety).

3.30 Độ tin cậy (Reliability)

Khả năng một hạng mục có thể thực hiện các chức năng được yêu cầu dưới các điều kiện đã định trong một khoảng thời gian cho trước (t_1, t_2). (IEC 60050(191)).

3.31 Gia tăng độ tin cậy (Reliability growth)

Trạng thái thể hiện sự gia tăng liên tục của đại lượng độ tin cậy của một hạng mục theo thời gian. (IEC 60050(191))

3.32 Sửa chữa (Repair)

Là các hoạt động bảo dưỡng khắc phục được thực hiện đối với một hạng mục (IEC 60050(191)).

3.33 Sự phục hồi (Restoration)

Là trạng thái một hạng mục lấy lại khả năng thực hiện chức năng cần thiết sau khi bị hư hỏng (IEC 60050(191)).

3.34 Rủi ro (Risk)

Tỉ lệ xuất hiện của một nguy hiểm gây ra thiệt hại và mức độ nghiêm trọng của thiệt hại đó.

3.35 Độ an toàn (Safety)

Trạng thái không tồn tại các rủi ro gây thiệt hại không thể chấp nhận được.

3.36 Hồ sơ an toàn (Safety case)

Tài liệu chứng minh sản phẩm phù hợp các yêu cầu an toàn được quy định.

3.37 Tính toàn vẹn về an toàn (Safety integrity)

Khả năng hệ thống thực hiện đầy đủ các chức năng an toàn đã được yêu cầu dưới tất cả các điều kiện đã biết trong một khoảng thời gian cho trước.

3.38 Mức toàn vẹn về an toàn (Safety integrity level (SIL))

Là một trị số quy định mức độ cụ thể các yêu cầu về tính toàn vẹn về an toàn của các chức năng an toàn được phân bổ cho các hệ thống liên quan tới an toàn. Mức toàn vẹn về an toàn (*Safety Integrity Level - SIL*) có trị số cao nhất sẽ có tính toàn vẹn về an toàn cao nhất.

3.39 Kế hoạch an toàn (Safety plan)

Là tài liệu ghi lại các hoạt động được tổ chức theo kế hoạch, các nguồn lực và các sự kiện để triển khai các cơ cấu tổ chức, thực hiện các trách nhiệm, các quy trình, các hoạt động, các khả năng và các nguồn

lực kết hợp với nhau để đảm bảo một hạng mục sẽ thỏa mãn các yêu cầu về an toàn cho trước liên quan tới hợp đồng hoặc dự án cho trước.

3.40 Cơ quan quản lý an toàn (Safety regulatory authority)

Là một cơ quan quản lý nhà nước chịu trách nhiệm cho việc xây dựng hoặc chấp thuận các yêu cầu về an toàn đối với đường sắt và đảm bảo hệ thống đường sắt thỏa mãn các yêu cầu.

3.41 Vòng đời hệ thống (System lifecycle)

Các hoạt động xuất hiện trong suốt khoảng thời gian bắt đầu khi hệ thống được khởi công và kết thúc khi hệ thống không còn khả năng sử dụng, ngừng hoạt động và hủy bỏ.

3.42 Hư hỏng có tính hệ thống (Systematic failures)

Các hư hỏng do các lỗi trong mọi vòng đời hệ thống an toàn trong mọi giai đoạn, gây ra hư hỏng do sự kết hợp cụ thể các đầu vào hoặc do một số điều kiện môi trường cụ thể.

3.43 Rủi ro chấp nhận được (Tolerable risk)

Mức độ lớn nhất về rủi ro của một sản phẩm có thể chấp nhận cho doanh nghiệp đường sắt.

3.44 Xác nhận (Validation)

Là việc kiểm tra và đưa ra các bằng chứng khách quan để đảm bảo các yêu cầu riêng đối với các mục đích sử dụng cụ thể được đáp ứng.

3.45 Thẩm tra (Verification)

Là việc bằng kiểm tra và đưa ra các bằng chứng khách quan để đảm bảo các yêu cầu cụ thể được đáp ứng.

CHÚ Ý: Để rõ ràng giữa thẩm tra (*verification)* và xác nhận (*validation)*, xem Hình 11 và mục 5.2.9.

4 RAMS đường sắt

4.1 Tổng quan

4.1.1 Điều này cung cấp các thông tin cơ sở về đối tượng của RAMS và kĩ thuật RAMS. Mục đích của điều này là cung cấp các thông tin cơ bản đầy đủ để có thể áp dụng hiệu quả tiêu chuẩn này cho các hệ thống đường sắt.

4.1.2 RAMS đường sắt đóng vai trò quan trọng trong Chất lượng Dịch vụ của Doanh nghiệp đường sắt. RAMS đường sắt được xác định bằng nhiều yếu tố thành phần; do đó, điều này được bố cục như sau:

1) Mục 4.2 xem xét mối quan hệ giữa RAMS đường sắt và chất lượng dịch vụ.

2) Từ mục 4.3 đến mục 4.8 xem xét các vấn đề của RAMS đường sắt:

- Các thành phần của RAMS;

- Các yếu tố ảnh hưởng và phương pháp để đạt được RAMS;

- Rủi ro và tính toàn vẹn về an toàn.

4.1.3 Trong mục này, các thuật ngữ sử dụng là thuật ngữ quốc tế nhưng những thuật ngữ mới được yêu cầu hoặc các thuật ngữ chuyên môn được xây dựng dành riêng cho lĩnh vực đường sắt được định nghĩa ở điều 3 của tiêu chuẩn này.

4.1.4 Trong phạm vi tiêu chuẩn này, các cụm từ “hệ thống, hệ thống con, tổng thành” được sử dụng để làm rõ sự phân chia mọi ứng dụng hoàn chỉnh thành các bộ phận cấu thành. Nghĩa chính xác của mỗi từ (hệ thống, hệ thống con và tổng thành) sẽ tùy thuộc các ứng dụng cụ thể.

4.1.5 Một hệ thống có thể được hình thành bằng sự lắp ghép các hệ thống con và các tổng thành, được liên kết với nhau theo một cách có tổ chức, để thực hiện chức năng cụ thể. Chức năng sẽ được quy định cho các hệ thống con và các tổng thành trong hệ thống và tình trạng hoạt động của hệ thống sẽ bị thay đổi nếu chức năng hệ thống con hoặc tổng thành thay đổi. Hệ thống sẽ xử lý các thông số đầu vào để tạo ra các đầu ra được quy định khi tương tác với môi trường.

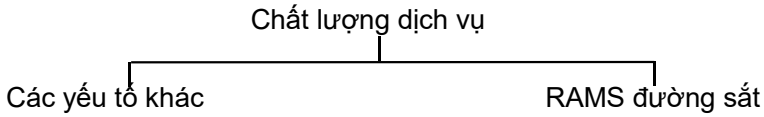
4.2 RAMS đường sắt và chất lượng dịch vụ

4.2.1 Mục này giới thiệu về mối liên hệ giữa RAMS và chất lượng dịch vụ cho một công việc.

4.2.2 RAMS là một đặc tính của quá trình vận hành dài hạn của một hệ thống và đạt được bằng cách áp dụng các khái niệm, phương pháp, công cụ và kĩ thuật công nghệ đã được xây dựng trong suốt vòng đời hệ thống của hệ thống. RAMS của một hệ thống có thể được mô tả bằng một chỉ số mức độ định tính hoặc định lượng mà ở đó hệ thống, hoặc các hệ thống con và các tổng thành có thể dựa vào đó để thực hiện các chức năng đã được quy định và đều sẵn sàng và an toàn. RAMS của hệ thống, trong nội dung của tiêu chuẩn này, là sự kết hợp của Độ tin cậy, tính sẵn sàng, khả năng bảo dưỡng và độ an toàn, RAMS.

4.2.3 Mục tiêu của hệ thống đường sắt là đạt được chỉ tiêu về vận tải đường sắt trong một khoảng thời gian cho trước một cách an toàn. RAMS đường sắt thể hiện mức độ tin cậy vào khả năng hệ thống

có thể bảo đảm đạt được mục tiêu trên. RAMS đường sắt có sự ảnh hưởng rõ ràng đến chất lượng khai thác dịch vụ cung cấp cho khách hàng. Chất lượng dịch vụ bị ảnh hưởng bởi các yếu tố khác liên quan tới chức năng và sự hoạt động, ví dụ như tần suất của khai thác, tính ổn định của dịch vụ và chi phí. Mối quan hệ này được thể hiện trong Hình 1.



Hình 1 – Chất lượng dịch vụ và RAMS đường sắt

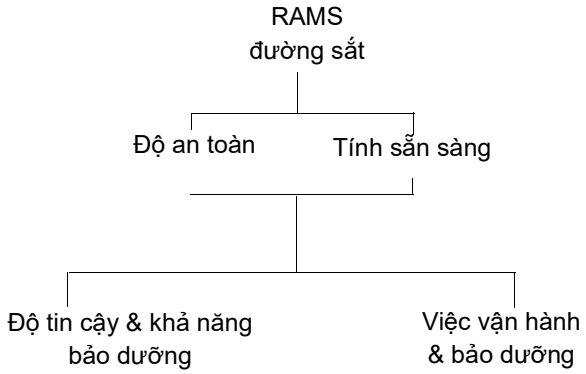
4.3 Các thành phần của RAMS đường sắt

4.3.1 Mục này chỉ ra sự tương tác giữa các yếu tố RAMS bao gồm độ tin cậy, tính sẵn sàng, khả năng bảo dưỡng và độ an toàn trong các hệ thống đường sắt.

4.3.2 Độ an toàn và tính sẵn sàng được liên kết qua lại với nhau, có nghĩa là sự yếu kém của một trong hai thành phần hoặc lỗi quản lý các xung đột giữa các yêu cầu về độ an toàn và tính sẵn sàng có thể ngăn cản sự hình thành một hệ thống đáng tin cậy. Sự liên kết qua lại giữa các yếu tố RAMS đường sắt, độ tin cậy, tính sẵn sàng và độ an toàn được đưa ra trong Hình 2.

4.3.3 Các mục tiêu về độ an toàn và tính sẵn sàng trong khai thác chỉ có thể đạt được khi tất cả các yêu cầu về độ an toàn và khả năng bảo dưỡng được đáp ứng, việc thực hiện các hoạt động bảo dưỡng vận hành đang diễn ra, trong dài hạn và môi trường hệ thống được kiểm soát.

4.3.4 An ninh có thể được coi như một yếu tố bổ sung của RAMS, nó mô tả khả năng thay đổi của một hệ thống đường sắt để chống lại sự phá hoại và các hành vi không hợp lý của con người. Tuy nhiên, việc xem xét tính an ninh nằm ngoài phạm vi của tiêu chuẩn này.



Hình 2 – Mối quan hệ qua lại giữa các yếu tố RAMS

4.3.5 Các khái niệm kĩ thuật của tính sẵn sàng được dựa trên sự hiểu biết về:

a) Độ tin cậy:

- Tất cả các dạng hư hỏng có thể của hệ thống trong các ứng dụng khai thác và môi trường quy định;

- Xác suất xuất hiện của từng hư hỏng hoặc tỉ lệ xuất hiện của từng hư hỏng;

- Tác động của hư hỏng đến chức năng của hệ thống;

b) Tính bảo dưỡng:

- Thời gian thực hiện việc bảo dưỡng có kế hoạch;

- Thời gian cho việc phát hiện, xác định lỗi và vị trí các lỗi;

- Thời gian cho việc hồi phục một hệ thống đã hư hỏng (bảo dưỡng không có kế hoạch);

c) Vận hành và bảo dưỡng:

- Tất cả các chế độ vận hành có thể xảy ra và hoạt động bảo dưỡng được yêu cầu trong toàn bộ vòng đời hệ thống của hệ thống;

- Các vấn đề liên quan tới yếu tố con người.

4.3.6 Các khái niệm kĩ thuật về an toàn dựa trên sự hiểu biết về:

a) Tất cả các nguy hiểm có thể tồn tại trong hệ thống, ở mọi chế độ vận hành, bảo dưỡng và hình thái môi trường.

b) Đặc tính về mức độ nghiêm trọng của hậu quả đối với từng nguy hiểm.

c) Lỗi về an toàn hoặc các hư hỏng liên quan tới an toàn đối với:

- Tất cả các dạng hư hỏng hệ thống mà có thể dẫn tới một nguy hiểm (các dạng hư hỏng liên quan tới an toàn). Đây là một tập hợp con trong tất cả các dạng hư hỏng về độ tin cậy (a));

- Xác suất xuất hiện của từng dạng hư hỏng hệ thống liên quan tới an toàn;

- Sự trùng hợp và/hoặc chuỗi liên tiếp các tình huống, các hư hỏng, các trạng thái vận hành, các điều kiện môi trường… trong hệ thống, mà có thể dẫn đến tai nạn (ví dụ: một nguy hiểm sẽ dẫn đến một tai nạn);

- Xác suất xuất hiện của từng tình huống, từng hư hỏng, từng trạng thái vận hành, từng điều kiện môi trường… trong hệ thống.

d) Khả năng bảo dưỡng của các bộ phận liên quan tới an toàn trong hệ thống về:

- Tính dễ dàng thực hiện các hoạt động bảo dưỡng các hạng mục hoặc các bộ phận liên quan tới an toàn của hệ thống hoặc các tổng thành của nó mà có liên quan tới nguy hiểm hoặc dạng hư hỏng về an toàn.

- Xác xuất xuất hiện các lỗi trong các hoạt động bảo dưỡng các bộ phận liên quan tới an toàn trong hệ thống;

- Thời gian để khôi phục hệ thống trở về trạng thái an toàn.

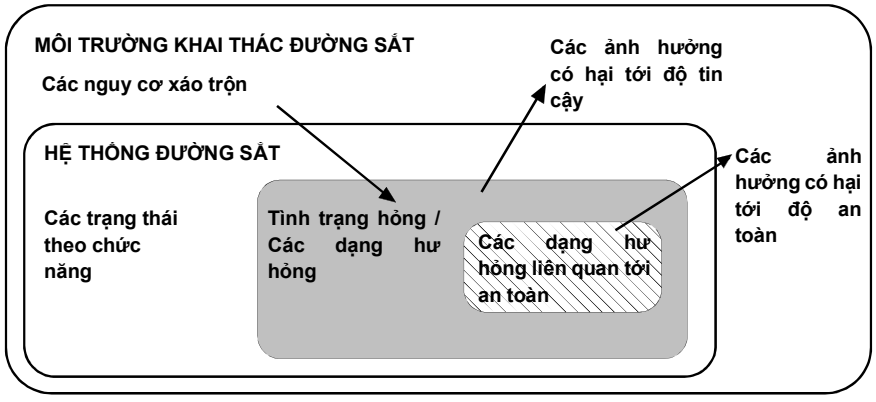
e) Sự vận hành và bảo dưỡng hệ thống của các bộ phận liên quan tới an toàn trong hệ thống đối với:

- Sự ảnh hưởng của các yếu tố con người trong các hoạt động bảo dưỡng có hiệu quả của tất cả các bộ phận liên quan tới an toàn của hệ thống và khả năng vận hành an toàn của hệ thống;

- Các công cụ, các thiết bị và các quy trình để vận hành an toàn và để bảo dưỡng hiệu quả các bộ phận liên quan tới an toàn của hệ thống;

- Các biện pháp kiểm soát hiệu quả để giải quyết nguy hiểm và giảm bớt các hậu quả của nó.

4.3.7 Các hư hỏng trong một hệ thống vận hành trong giới hạn của một hệ thống và môi trường sẽ có tác động lên sự hoạt động của hệ thống. Tất cả các hư hỏng sẽ tác động có hại lên độ tin cậy của hệ thống, tuy nhiên chỉ một số hư hỏng cụ thể tác động có hại đến an toàn trong phạm vi hệ thống cụ thể. Môi trường cũng có thể ảnh hưởng tới chức năng của hệ thống và tiếp đến là độ an toàn của các hoạt động hệ thống đường sắt. Những mối liên hệ này được thể hiện như trong Hình 3.



Hình 3 – Các tác động của hư hỏng trong một hệ thống

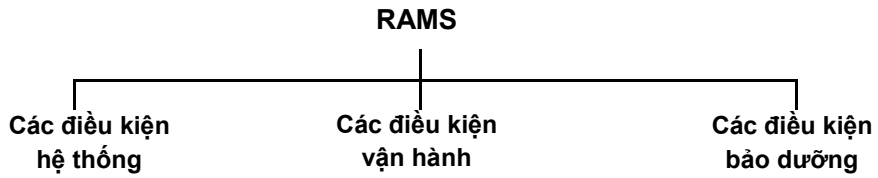
4.3.8 Một hệ thống đường sắt đáng tin cậy chỉ có thể được nhận biết thông qua việc xem xét chỉ dẫn kĩ thuật, tương tác giữa các yếu tố RAMS trong hệ thống và kết quả từ việc kết hợp tối ưu RAMS cho hệ thống.

4.4 Các yếu tố ảnh hưởng tới RAMS đường sắt

4.4.1 Tổng quan

4.4.1.1 Mục này giới thiệu và quy định quy trình hỗ trợ việc xác định các yếu tố ảnh hưởng tới RAMS của các hệ thống đường sắt, cùng với việc xem xét cụ thể sự ảnh hưởng của các yếu tố con người. Những yếu tố này cùng với ảnh hưởng của nó sẽ là đầu vào cho việc quy định các yêu cầu về RAMS đối với các hệ thống.

4.4.1.2 RAMS của hệ thống đường sắt bị ảnh hưởng bởi ba nguồn gây hư hỏng: nguồn gây hư hỏng phát sinh từ bên trong hệ thống tại bất kì giai đoạn nào của vòng đời hệ thống (các điều kiện hệ thống); nguồn gây hư hỏng xuất hiện trong hệ thống khi vận hành (các điều kiện vận hành); và nguồn gây hư hỏng xuất hiện trong hệ thống khi tiến hành bảo dưỡng (các điều kiện bảo dưỡng). Những nguồn gây hư hỏng này có thể tương tác với nhau. Mối liên hệ này được thể hiện trong Hình 4 và chi tiết trong Hình 5.



Hình 4 - Ảnh hưởng lên RAMS

4.4.1.3 Để nhận biết các hệ thống đáng tin cậy, thì các yếu tố có thể ảnh hưởng tới RAMS của hệ thống cần phải được xác định, các tác động của chúng cần được đánh giá và nguyên nhân của những tác động này cần được quản lý trong suốt vòng đời hệ thống của hệ thống bằng việc áp dụng các biện pháp kiểm soát phù hợp nhằm tối ưu hóa sự hoạt động của hệ thống.

4.4.2 Phân loại các yếu tố

4.4.2.1 Mục này nêu chi tiết về quy trình xác định các yếu tố sẽ ảnh hưởng tới mục tiêu hệ thống thỏa mãn các yêu cầu về RAMS đã xác định trước đó.

4.4.2.2 Ở mức độ ban đầu, các yếu tố ảnh hưởng tới RAMS hệ thống là tổng quát, áp dụng chung cho tất cả các hệ thống công nghiệp. Hình 5 thể hiện một số các yếu tố phổ biến ảnh hưởng tới RAMS của hệ thống giao thông vận tải và mối tương tác giữa những yếu tố này. Để xác định các yếu tố chi tiết ảnh

hưởng tới RAMS của các hệ thống đường sắt, mỗi yếu tố ảnh hưởng trên phải được xem xét trong phạm vi của một hệ thống cụ thể.

4.4.2.3 Việc phân tích các yếu tố con người về tác động của con người đến RAMS hệ thống sẽ có trong "phương pháp hệ thống" được quy định trong tiêu chuẩn này.

4.4.2.4 Các yếu tố con người có thể được xác định bởi tác động của tính cách con người, mong muốn và hành vi lên hệ thống. Những yếu tố này bao gồm các vấn đề về hình thể, thể chất và tâm lý của con người. Các yếu tố trên được sử dụng để giúp con người thực hiện công việc hiệu quả và năng suất, có tính đến nhu cầu của con người về các vấn đề như sức khỏe, an toàn và sự hài lòng với công việc.

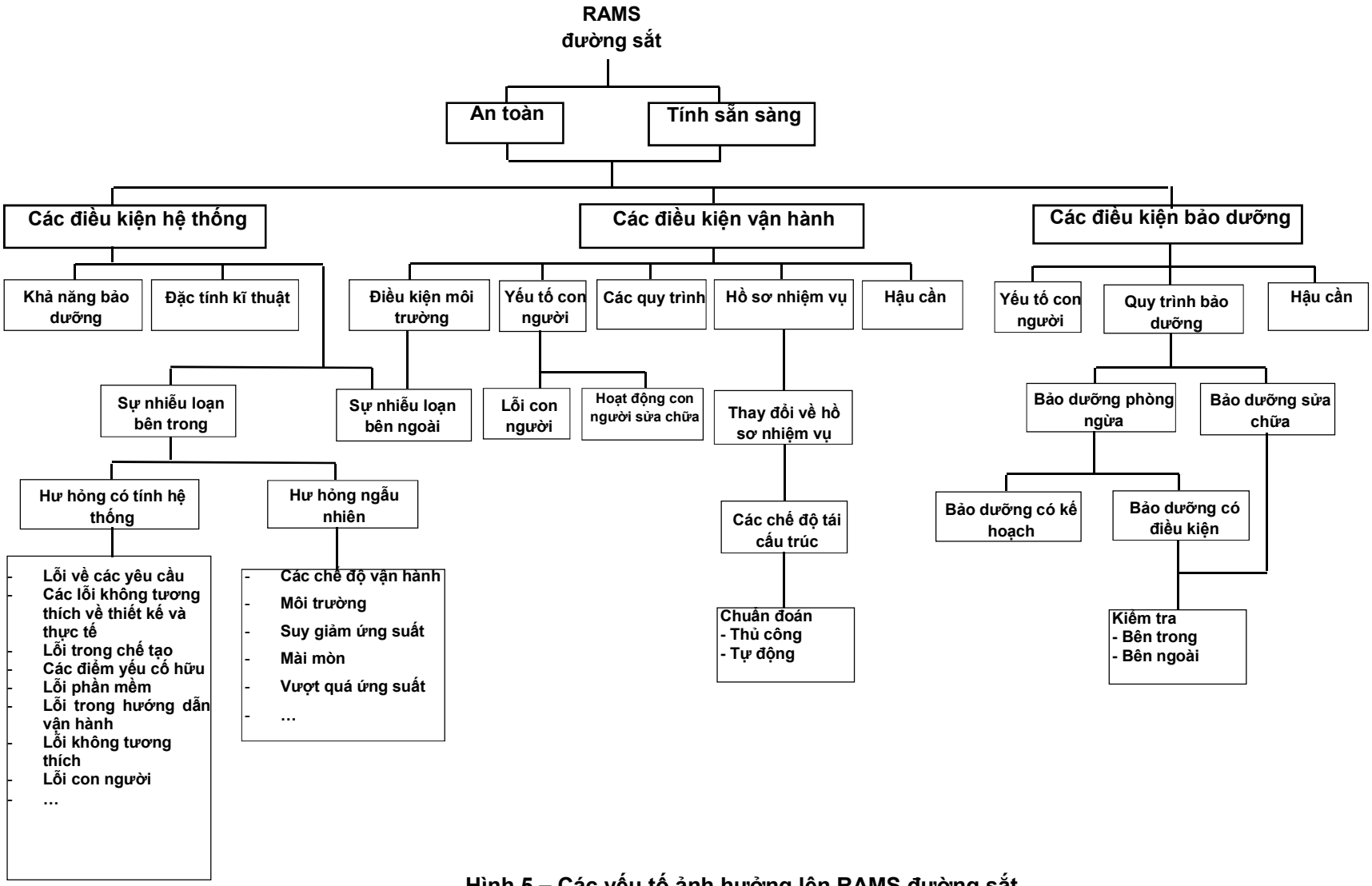
4.4.2.5 Các hệ thống đường sắt liên quan chủ yếu tới một phạm vi rộng các nhóm người, từ hành khách, nhân viên vận hành và nhân viên điều hành các hệ thống đến các nhóm người bị ảnh hưởng bởi sự hoạt động của hệ thống đường sắt, như lái xe ô tô ở các đường ngang giao cắt. Mỗi nhóm người có khả năng phản ứng lại với các tình huống theo các cách khác nhau. Rõ ràng, tác động tiềm ẩn của con người lên RAMS của hệ thống đường sắt là rất lớn. Do đó, việc đạt được RAMS đường sắt sẽ yêu cầu việc kiểm soát các yếu tố con người chặt chẽ hơn trong suốt toàn bộ vòng đời hệ thống của hệ thống, hơn các yêu cầu trong nhiều ứng dụng công nghiệp khác.

4.4.2.6 Con người phải được coi như là yếu tố có khả năng ảnh hưởng tích cực tới RAMS của hệ thống đường sắt. Để đạt được mục đích này, cách thức mà các yếu tố con người có thể ảnh hưởng tới RAMS đường sắt nên được xác định và quản lý trong suốt toàn bộ vòng đời hệ thống. Phân tích này nên bao gồm tác động tiềm ẩn của các yếu tố con người lên RAMS đường sắt trong các giai đoạn thiết kế và xây dựng hệ thống.

4.4.2.7 Trong khi yêu cầu về các yếu tố con người trong vòng đời hệ thống là tổng quát chung, thì ảnh hưởng chính xác của các yếu tố con người lên RAMS sẽ là cụ thể đối với hệ thống đường sắt được xem xét.

4.4.2.8 Các yếu tố chung bao gồm các thành phần có trong Hình 5 nên được đánh giá trong phạm vi của hệ thống đường sắt. Doanh nghiệp đường sắt phải quy định rõ các yếu tố không được áp dụng khi mời thầu. Từng yếu tố chung có thể áp dụng phải được đánh giá và nêu chi tiết các yếu tố ảnh hưởng cụ thể với từng hệ thống đường sắt và được rút ra một cách có hệ thống. Các vấn đề về yếu tố con người, mà ảnh hưởng chính tới quy trình quản lý RAMS tích hợp, phải được đề cập trong quá trình đánh giá này.

4.4.2.9 Để rút ra được các yếu tố ảnh hưởng chi tiết, phải sử dụng hai danh sách nội dung kiểm tra bao quát được các yếu tố đường sắt cụ thể (4.4.2.10) và các yếu tố con người (4.4.2.11), hoặc bằng sự thể hiện thay thế như trong Hình 5.



Hình 5 – Các yếu tố ảnh hưởng lên RAMS đường sắt

4.4.2.10 Việc rút ra chi tiết các yếu tố ảnh hưởng cụ thể lên hệ thống đường sắt nên có sự xem xét nhưng không bị giới hạn vào từng yếu tố đường sắt cụ thể dưới đây. Chú ý danh sách kiểm tra dưới đây là chưa đủ và nên được thay đổi cho phù hợp với phạm vi và mục đích của hệ thống:

a) Vận hành hệ thống:

- Các nhiệm vụ mà hệ thống phải thực hiện và các điều kiện để thực hiện các nhiệm vụ đó;
- Sự tồn tại đồng thời hành khách, hàng hóa, nhân viên và các hệ thống trong môi trường vận hành;
- Các yêu cầu về tuổi thọ của hệ thống, bao gồm sự kì vọng vào tuổi thọ hệ thống, mật độ khai thác và các yêu cầu về chi phí vòng đời hệ thống.

b) Môi trường:

- Môi trường vật lý;
- Mức độ tích hợp cao của các hệ thống đường sắt trong môi trường;
- Khả năng thử nghiệm các hệ thống hoàn chỉnh trong môi trường đường sắt ở mức độ giới hạn.

c) Các điều kiện sử dụng:

- Các ràng buộc phát sinh từ kết cấu hạ tầng và các hệ thống hiện tại lên hệ thống mới;
- Nhu cầu duy trì các dịch vụ đường sắt trong các nhiệm vụ có trong vòng đời hệ thống.

d) Các điều kiện vận hành:

- Các điều kiện lắp đặt trên tuyến;
- Các điều kiện bảo dưỡng trên tuyến;
- Mức độ tích hợp các hệ thống hiện có và các hệ thống mới trong quá trình thử hoạt động và vận hành.

e) Phân loại hư hỏng:

- Các tác động của hư hỏng trong một hệ thống con.

4.4.2.11 Việc rút ra chi tiết các yếu tố ảnh hưởng cụ thể tới con người nên có sự xem xét nhưng không bị giới hạn vào từng yếu tố con người dưới đây. Chú ý danh sách kiểm tra dưới đây không phải là đầy đủ và nên được thay đổi cho phù hợp với phạm vi và mục đích của hệ thống đường sắt.

a) Việc bố trí các chức năng hệ thống giữa con người và máy móc.

b) Ảnh hưởng lên hoạt động con người trong hệ thống từ:

- Tương tác giữa con người với hệ thống;
- Môi trường, bao gồm môi trường vật lý và các yêu cầu về công thái học;
- Tính chất công việc;
- Năng lực của con người;
- Quá trình xây dựng nhiệm vụ cho con người;
- Sự phối hợp công việc giữa con người;
- Quá trình phản hồi của con người;
- Cơ cấu tổ chức của đường sắt;
- Văn hóa đường sắt;
- Thuật ngữ chuyên ngành đường sắt;
- Các vấn đề phát sinh từ việc áp dụng công nghệ mới.

c) Các yêu cầu đối với hệ thống phát sinh từ:

- Năng lực của con người;
- Động lực và tạo cảm hứng cho con người;
- Sự giảm bớt các tác động của việc thay đổi thái độ làm việc của con người;
- Các công tác bảo vệ an toàn vận hành;
- Thời gian và không gian cho phản ứng của con người.

d) Các yêu cầu đối với hệ thống phát sinh từ khả năng xử lý thông tin của con người, bao gồm:

- Giao tiếp giữa con người với máy móc;
- Mật độ truyền tải thông tin;
- Tốc độ truyền tải thông tin;

- Chất lượng thông tin;
- Phản ứng của con người với các tình huống bất bình thường;
- Đào tạo nhân lực;
- Hỗ trợ quá trình đưa ra các quyết định của con người;
- Các yếu tố khác dẫn đến sự mệt mỏi của con người.

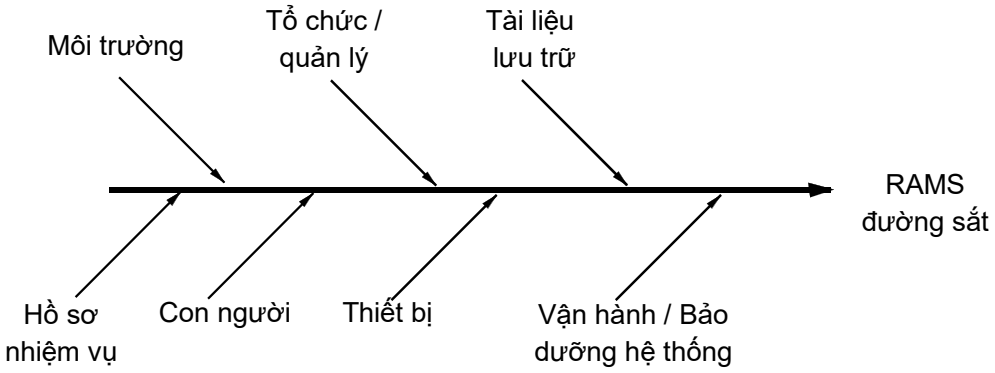
e) Tác động của các yếu tố tương giao con người/hệ thống lên hệ thống, bao gồm:

- Thiết kế và sự vận hành của các tương giao con người/hệ thống;
- Tác động của lỗi con người;
- Tác động từ sự vi phạm nguyên tắc cố ý của con người;
- Sự liên quan và sự can thiệp của con người trong hệ thống;
- Giám sát và quyền kiểm soát hệ thống của con người;
- Nhận thức của con người về rủi ro;
- Sự liên quan của con người trong các bộ phận quan trọng của hệ thống;
- Khả năng để dự đoán trước các vấn đề hệ thống của con người.

f) Các yếu tố con người trong thiết kế và xây dựng hệ thống, bao gồm:

- Năng lực của lỗi do con người;
- Sự độc lập của con người trong thiết kế;
- Sự liên quan của con người trong quá trình thẩm tra và xác nhận;
- Tương giao giữa con người và các công cụ tự động hóa;
- Các quá trình phòng ngừa hư hỏng mang tính hệ thống.

4.4.2.12 Khuyến nghị sử dụng cách tiếp cận bằng sơ đồ để rút ra các yếu tố chi tiết, như sơ đồ nguyên nhân/hậu quả. Ví dụ về một sơ đồ nguyên nhân/hậu quả đơn giản hóa được thể hiện trong Hình 6.



Hình 6 – Ví dụ về sơ đồ Nguyên nhân / Hệ quả

4.4.3 Quản lý các yếu tố

Tác động tiềm ẩn của mỗi yếu tố ảnh hưởng lên RAMS hệ thống đường sắt phải được đánh giá ở mức độ phù hợp với hệ thống được xem xét. Việc đánh giá này phải bao gồm cả sự xem xét tác động của mỗi yếu tố ở mỗi một giai đoạn trong vòng đời hệ thống và phải ở mức phù hợp với hệ thống được xem xét. Việc đánh giá này cũng phải đề cập tới sự tương tác của các yếu tố ảnh hưởng liên quan. Đối với các yếu tố liên quan tới con người, việc đánh giá phải xem xét tác động của từng yếu tố trong mối liên quan lẫn nhau.

4.5 Phương pháp để đạt được các yêu cầu về RAMS đường sắt

4.5.1 Tổng quan

4.5.1.1 Phương pháp để đạt được các yêu cầu về RAMS đường sắt sẽ liên quan tới việc kiểm soát các yếu tố ảnh hưởng tới RAMS trong suốt vòng đời hệ thống của hệ thống. Việc kiểm soát hiệu quả yêu cầu cần thiết lập các cơ chế và các quy trình để phòng ngừa các nguồn tác động gây lỗi phát sinh trong quá trình đưa hệ thống vào hoạt động và hỗ trợ hệ thống hoạt động. Việc phòng ngừa cũng cần phải tính tới cả các hư hỏng ngẫu nhiên và hư hỏng có tính hệ thống.

4.5.1.2 Các phương pháp được sử dụng để đạt được các yêu cầu về RAMS sẽ dựa trên nhận thức về cách áp dụng các biện pháp phòng ngừa để giảm thiểu tối đa khả năng xuất hiện hư hỏng do lỗi trong các giai đoạn vòng đời hệ thống. Các biện pháp phòng ngừa là sự kết hợp của:

a) Phòng ngừa: liên quan tới việc giảm bớt xác xuất hư hỏng;

b) Bảo vệ: liên quan tới việc giảm bớt mức độ nghiêm trọng của hậu quả hư hại.

4.5.1.3 Phải chứng minh chiến lược để đạt được các yêu cầu về RAMS cho hệ thống, bao gồm cả việc sử dụng các phương pháp phòng ngừa và/hoặc bảo vệ.

4.5.2 Quy định RAMS

4.5.2.1 Việc quy định các yêu cầu về RAMS là một quá trình phức tạp. Phụ lục A của tiêu chuẩn này đưa ra một ví dụ tóm tắt quy định các yêu cầu về RAMS dựa trên quy trình được nêu chi tiết trong tiêu chuẩn này. Phụ lục B của tiêu chuẩn này đưa ra một ví dụ tóm tắt quy trình xác định chương trình RAMS dựa trên các yêu cầu của tiêu chuẩn này. Cả hai phụ lục mang tính tham khảo đều chỉ dùng để hướng dẫn và được phổ biến, ví dụ về phương tiện giao thông đường sắt.

Phụ lục B cũng đưa ra danh sách các công cụ phù hợp cho việc phân tích RAMS. Việc lựa chọn một công cụ phù hợp sẽ dựa trên hệ thống được xem xét và các yếu tố như tính quan trọng, tính mới lạ, mức độ phức tạp… của hệ thống

4.5.2.2 Bảng 1 xác định các loại hư hỏng RAM phù hợp được sử dụng trong các hệ thống đường sắt.

Bảng 1 – Phân loại hư hỏng RAM

Phân loại hư hỏng	Định nghĩa
Nghiêm trọng (Hư hỏng không thể di chuyển)	Là hư hỏng: - Làm cho đoàn tàu không thể di chuyển hoặc gây ra sự chậm trễ đối với việc khai thác lớn hơn so với thời gian được quy định và /hoặc phát sinh ra chi phí lớn hơn so với mức quy định
Chính (Hư hỏng trong khai thác)	Là hư hỏng: - Phải được sửa chữa để hệ thống đạt được sự hoạt động quy định và - Không gây ra sự chậm trễ hoặc chi phí lớn hơn định mức được quy định cho một hư hỏng nghiêm trọng.
Nhỏ	Là hư hỏng: - Không cản trở hệ thống đạt được sự hoạt động được quy định và - Không đáp ứng chỉ tiêu cho các hư hỏng nghiêm trọng hoặc hư hỏng chính.

4.5.2.3 Các thông số phù hợp để mô tả độ tin cậy, tính sẵn sàng, khả năng bảo dưỡng, nguồn lực cung ứng và các yêu cầu về an toàn của các hệ thống đường sắt được thể hiện trong Phụ lục C (tham khảo). Các thông số cụ thể sẽ dựa trên hệ thống được xem xét. Tất cả các thông số về RAMS được sử dụng nên được thỏa thuận giữa Doanh nghiệp đường sắt và các đơn vị cung ứng phụ trợ đường sắt. Khi các thông số có thể được thể hiện bằng các đơn vị khác thay thế thì phải đưa ra các hệ số chuyển đổi.

4.6 Rủi ro

4.6.1 Khái niệm về rủi ro

Khái niệm về rủi ro là sự kết hợp của hai yếu tố:

- Xác suất của sự xuất hiện một tình huống hoặc của sự kết hợp các tình huống dẫn đến một nguy hiểm, hoặc tần suất của những xuất hiện này;

- Hậu quả của nguy hiểm

4.6.2 Phân tích rủi ro

4.6.2.1 Phân tích rủi ro phải được thực hiện ở các giai đoạn khác nhau trong vòng đời hệ thống của hệ thống bởi đơn vị chịu trách nhiệm cho giai đoạn đó và phải được lưu lại trong hồ sơ. Việc lập hồ sơ phải bao gồm tối thiểu những nội dung dưới đây:

a) Phương pháp phân tích;

b) Các giả thuyết, các giới hạn và căn cứ của phương pháp sử dụng;

c) Các kết quả của việc xác định các nguy hiểm;

d) Các kết quả của việc đánh giá nguy hiểm và độ tin cậy của công việc này;

e) Các kết quả của các nghiên cứu sẵn có;

f) Dữ liệu, nguồn thông tin và mức độ tin cậy;

g) Các tài liệu tham khảo.

4.6.2.2 Theo quan điểm định tính, Bảng 2 đưa ra các phân loại đặc trưng về xác suất hoặc tần suất xuất hiện các tình huống nguy hiểm và mô tả cho từng loại đối với hệ thống đường sắt. Các loại, giá trị của chúng và giá trị quy đổi áp dụng phải được Doanh nghiệp đường sắt quy định, phù hợp với hệ thống đường sắt được xem xét.

Bảng 2 – Tần suất xuất hiện của các tình huống nguy hiểm

Phân loại	Mô tả
Thường xuyên	Có khả năng xuất hiện thường xuyên. Nguy hiểm sẽ xảy ra liên tục
Có khả năng	Sẽ xuất hiện một số lần. Nguy hiểm có thể được coi như xuất hiện thường xuyên
Đôi khi	Có khả năng xuất hiện một vài lần. Nguy hiểm có thể được coi như xuất hiện một số lần
Hiếm khi	Có khả năng thỉnh thoảng xuất hiện trong vòng đời hệ thống. Nguy hiểm có thể được coi như xuất hiện có lý do
Khó có khả năng	Ít có khả năng xuất hiện nhưng có thể. Có thể xem như nguy hiểm xuất hiện một cách đặc biệt.
Không thể xuất hiện	Không có khả năng xuất hiện. Có thể giả thiết rằng nguy hiểm gần như không xuất hiện

4.6.2.3 Phân tích hậu quả phải được sử dụng để đánh giá các tác động có thể xảy ra. Bảng 3 mô tả các mức độ nghiêm trọng điển hình của các hư hỏng và các hậu quả đi kèm cho từng mức độ đối với tất cả các hệ thống đường sắt. Doanh nghiệp đường sắt quy định giá trị mức độ nghiêm trọng và các hậu quả cho từng mức độ nghiêm trọng được áp dụng, phù hợp với hệ thống đường sắt được xem xét.

Bảng 3 – Mức độ nghiêm trọng của nguy hiểm

Mức độ nghiêm trọng	Hệ quả đối với con người và môi trường	Hệ quả đối với khai thác
Thảm họa	Nhiều người bị tử vong và/hoặc nhiều người bị chấn thương nặng và/hoặc các phá hoại nghiêm trọng về môi trường	
Nghiêm trọng	Một tử vong và/hoặc chấn thương nặng và/hoặc phá hoại đáng kể về môi trường	Thiệt hại hệ thống quan trọng
Bình thường	Chấn thương nhẹ và/hoặc đe dọa đáng kể về môi trường	Hư hại nặng đối với các hệ thống
Không đáng kể	Chấn thương nhẹ có thể xảy ra	Hư hại nhẹ đối với hệ thống

4.6.3 Đánh giá và chấp nhận rủi ro

4.6.3.1 Mục này quy định việc lập ma trận "tần suất – hậu quả" để đánh giá các kết quả phân tích rủi ro, xếp hạng rủi ro, các hoạt động giảm bớt rủi ro hoặc loại bỏ các rủi ro không chấp nhận được; và để chấp nhận rủi ro.

4.6.3.2 Việc đánh giá rủi ro phải được thực hiện bằng việc kết hợp tần suất xuất hiện của tình huống có tính nguy hiểm tương ứng với mức độ nghiêm trọng của nó để thiết lập mức độ rủi ro cho tình huống nguy hiểm. Một ma trận "tần suất – hậu quả" được thể hiện trong Bảng 4.

Bảng 4 – Ma trận tần suất – hậu quả

Tần suất xuất hiện của tình huống nguy hiểm	**Mức độ rủi ro**			
Thường xuyên				
Có khả năng				
Đôi khi				
Hiếm khi				
Khó có khả năng				
Không thể xuất hiện				
	Không đáng kể	Bình thường	Nghiêm trọng	Thảm họa
	Mức độ nghiêm trọng của hậu quả nguy hiểm			

4.6.3.3 Việc chấp nhận rủi ro phải dựa trên một nguyên tắc chấp nhận chung. Có thể sử dụng một số nguyên tắc sẵn có. Một số ví dụ như dưới đây: (xem thêm phụ lục D để tham khảo các nguyên tắc này)

- Nguyên tắc thấp đến mức hợp lý (Nguyên tắc ALARP);

- Nguyên tắc rủi ro tổng thể càng thấp càng tốt (Nguyên tắc GAMAB). Công thức hoàn chỉnh cho nguyên tắc này là "Tất cả các hệ thống giao thông vận tải dẫn hướng mới phải có một mức độ rủi ro tổng thể tối thiểu bằng mức độ của hệ thống sẵn có tương đương";

- Tỉ lệ tử vong nội sinh nhỏ nhất (nguyên tắc MEM).

Bảng 5 quy định các mức độ rủi ro định tính và các hoạt động được áp dụng theo từng mức độ. Doanh nghiệp đường sắt phải chịu trách nhiệm cho việc xác định nguyên tắc sử dụng phù hợp, mức độ rủi ro chấp nhận được và các mức độ nằm trong các phân loại rủi ro khác nhau.

Bảng 5 – Phân loại rủi ro định tính

Mức rủi ro	Các hoạt động được áp dụng theo các mức
Không chấp nhận được	Phải bị loại bỏ
Không mong muốn	Chỉ được chấp nhận khi việc giảm rủi ro không thể thực hiện được thêm nữa và có sự đồng ý của Doanh nghiệp đường sắt hoặc cơ quan quản lý về an toàn, nếu phù hợp
Chấp nhận được	Có thể chấp nhận được với các kiểm soát đầy đủ và có sự đồng ý của Doanh nghiệp đường sắt
Có thể bỏ qua	Chấp nhận được mà có/không cần có sự đồng ý của Doanh nghiệp đường sắt

4.6.3.4 Bảng 6 đưa ra ví dụ về đánh giá rủi ro và giảm bớt/kiểm soát rủi ro để chấp nhận rủi ro.

Bảng 6 – Ví dụ về đánh giá và chấp nhận rủi ro

*Tần suất xuất hiện của tình huống nguy hiểm	Mức độ rủi ro			
Thường xuyên	Không mong muốn	Không chấp nhận được	Không chấp nhận được	Không chấp nhận được
Có khả năng	Chấp nhận được	Không mong muốn	Không chấp nhận được	Không chấp nhận được
Đôi khi	Chấp nhận được	Không mong muốn	Không mong muốn	Không chấp nhận được
Hiếm khi	Có thể bỏ qua	Chấp nhận được	Không mong muốn	Không mong muốn
Khó có khả năng	Có thể bỏ qua	Có thể bỏ qua	Chấp nhận được	Chấp nhận được
Không thể xuất hiện	Có thể bỏ qua	Có thể bỏ qua	Có thể bỏ qua	Có thể bỏ qua
	Không đáng kể	Bình thường	Nghiêm trọng	Thảm họa
	Mức độ nghiêm trọng của hậu quả nguy hiểm			

*Giá trị quy đổi đối với tần suất xuất hiện của các tình huống nguy hiểm sẽ dựa trên hệ thống đường sắt được xem xét (4.6.2.2)

Đánh giá rủi ro	Kiểm soát/giảm thiểu rủi ro
Không chấp nhận được	Phải bị loại bỏ
Không mong muốn	Chỉ chấp nhận khi việc giảm rủi ro không thể thực hiện được thêm nữa và có sự đồng ý của doanh nghiệp đường sắt
Chấp nhận được	Có thể chấp nhận được với các kiểm soát đầy đủ và có sự đồng ý của doanh nghiệp đường sắt

Có thể bỏ qua	Chấp nhận được mà không cần sự đồng ý của doanh nghiệp đường sắt

4.7 Tính toàn vẹn về an toàn

4.7.1 Khi mức độ an toàn đối với hệ thống được thiết lập và quá trình giảm bớt rủi ro cần thiết được đánh giá, thì có thể đưa ra các yêu cầu tính toàn vẹn về an toàn đối với các hệ thống và các tổng thành của hệ thống dựa trên các kết quả của quá trình đánh giá rủi ro. Tính toàn vẹn về an toàn có thể được xem như là sự kết hợp của các yếu tố có thể định lượng (thường kết hợp vào trong các phần cứng, như các hư hỏng ngẫu nhiên) và các yếu tố không thể định lượng (thường được kết hợp vào trong các hư hỏng có hệ thống trong phần mềm, các quy định, các tài liệu, các quy trình…). Các công cụ giảm bớt rủi ro bên ngoài và các biện pháp giảm bớt rủi ro hệ thống nên phù hợp với việc giảm bớt rủi ro cần thiết cho hệ thống để đạt được mức an toàn mục tiêu.

4.7.2 Độ tin cậy trong quá trình xác định tính toàn vẹn về an toàn của một chức năng trong hệ thống có thể đạt được thông qua việc áp dụng hiệu quả sự kết hợp các yếu tố cấu trúc, các phương pháp, các công cụ và kĩ thuật cụ thể. Tính toàn vẹn về an toàn sẽ tương quan với xác suất của hư hỏng để đạt được chức năng an toàn được yêu cầu. Các chức năng có nhiều yêu cầu về tính toàn vẹn hơn sẽ có khả năng cần nhiều chi phí hơn để xác định. Mặc dù có chú ý về một mối tương quan tổng quát được quy định trong tiêu chuẩn IEC 61508, nhưng tiêu chuẩn này không quy định mối tương quan giữa tính toàn vẹn về an toàn và các xác suất hư hỏng đối với các hệ thống đường sắt. Việc xác định mối tương quan cho các hệ thống đường sắt là trách nhiệm của Doanh nghiệp đường sắt. Tuy nhiên, quy trình quản lý được quy định trong tiêu chuẩn này là tổng quát và phù hợp để sử dụng với mọi mối tương quan, khi được đơn vị có thẩm quyền đồng ý hoặc được các doanh nghiệp đường sắt cùng thống nhất.

4.7.3 Các chức năng về an toàn có trong các hệ thống nên được thực hiện có sử dụng cấu trúc, các phương pháp, các công cụ và các kĩ thuật được quy định trong các tiêu chuẩn chi tiết liên quan khác. Ví dụ: EN 50128 quy định các phương pháp, các công cụ và các kĩ thuật để xây dựng các hệ thống phần mềm và EN 50129 quy định quy trình chấp nhận và phê duyệt các hệ thống tín hiệu điện tử đường sắt.

4.7.4 Tính toàn vẹn về an toàn được quy định một cách cơ bản cho các chức năng an toàn. Các chức năng an toàn nên được chỉ định cho các hệ thống an toàn và/hoặc cho các biện pháp giảm bớt rủi ro bên ngoài. Quy trình chỉ định này là lặp đi lặp lại, để tối ưu hóa thiết kế và chi phí cho toàn bộ hệ thống.

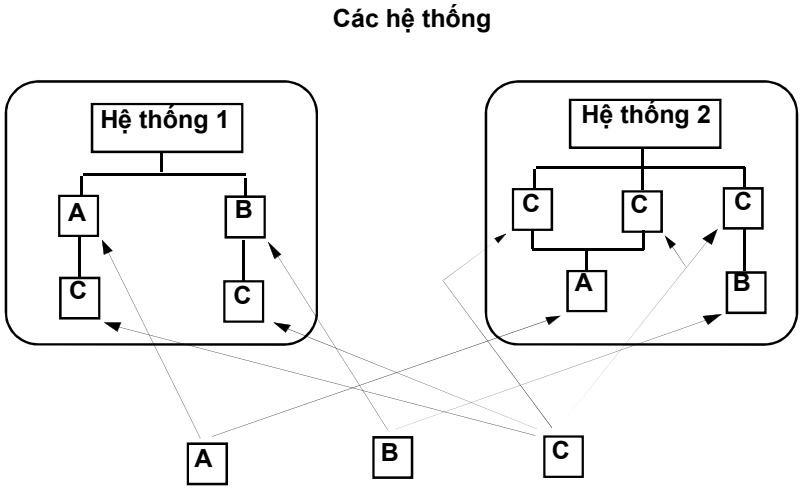
4.7.5 Khi được thực hiện một cách hiệu quả, Kế hoạch an toàn (*Safety Plan*) và Chương trình RAM sẽ đưa ra độ tin cậy đối với khả năng thỏa mãn các yêu cầu RAMS của hệ thống cuối cùng.

4.7.6 Nên chú ý các điểm dưới đây liên quan tới tính toàn vẹn về an toàn sản phẩm:

a) Chức năng an toàn được yêu cầu cho một hệ thống và tính toàn vẹn về an toàn tương ứng sẽ bị ảnh hưởng bởi môi trường hệ thống được sử dụng.

b) Khi một sản phẩm được xây dựng sử dụng các phương pháp, các công cụ và các kĩ thuật phù hợp đối với một mức độ cụ thể về tính toàn vẹn về an toàn, có thể đưa ra các tuyên bố rằng sản phẩm là có mức "X" về tính toàn vẹn về an toàn. Tuyên bố này nghĩa là sản phẩm sẽ thể hiện chức năng cụ thể trong môi trường xác định ở một mức toàn vẹn nhất định.

c) Hình 7 trình bày việc sử dụng các sản phẩm thương mại "chế tạo sẵn được bán đại trà" có thể khác nhau trong các hệ thống khác nhau. Ví dụ: sản phẩm A đang được sử dụng để thực hiện các chức năng khác nhau trong các hệ thống 1 và 2. Kết quả là tính toàn vẹn về an toàn yêu cầu cho sản phẩm có thể khác nhau giữa các hệ thống. Vì vậy, trước khi sử dụng một sản phẩm vào trong một hệ thống bất kì, các giới hạn và các ràng buộc áp dụng đối với chức năng và môi trường được tuyên bố của sản phẩm nên được đánh giá để đảm bảo rằng chúng phù hợp với các yêu cầu tổng thể của hệ thống.



Hình 7 – Các sản phẩm được chứng nhận trong các hệ thống an toàn

4.7.7 Trước khi áp dụng khái niệm về SIL, các yêu cầu dưới đây nên được xem xét:

a) Mức độ áp dụng SIL phù hợp nên được các chuyên gia về an toàn xây dựng. Khuyến nghị không sử dụng nhiều hơn 4 cấp độ.

b) Một SIL chỉ được áp dụng cho một "phần tử", là một thiết bị độc lập thực hiện một hoặc nhiều chức năng đơn giản và có thể được thay thế bởi thiết bị khác thực hiện cùng (các) chức năng. Nói chung, "phần tử" này thường là thiết bị mức thấp nhất và có thể được thay thế trong quá trình bảo dưỡng sửa chữa cấp đầu tiên.

c) Cho tới khi môi trường sản phẩm được đưa vào vẫn được coi là vô cùng quan trọng, phải kiểm tra mức độ giá trị SIL của sản phẩm thương mại được chứng nhận và phương pháp chứng nhận khi

được so sánh với các yêu cầu an toàn của nó để kết luận liệu tất cả các điều kiện có được đáp ứng cho hệ thống đang nghiên cứu.

d) Một SIL chỉ đề cập tới một mức độ được mong đợi về độ tin cậy đối với an toàn của một sản phẩm. Như được giải thích trong mục 4.3 của tiêu chuẩn này, các yêu cầu về an toàn và tính sẵn sàng sẽ tương quan qua lại trong hệ thống giao thông đường sắt. Khái niệm SIL không bao quát tất cả các mặt của một hệ thống và do đó việc chỉ xem xét một mình SIL có thể là không đủ (ví dụ: các chế độ vận hành xuống cấp hoặc các tình trạng hư hỏng cùng với các yêu cầu an toàn khác nhau...).

4.8 Khái niệm an toàn khi có sự cố (Fail-safe concept)

4.8.1 Tiêu chuẩn này sử dụng một phương pháp quản lý rủi ro mở rộng đối với an toàn. Phương pháp này là thống nhất với khái niệm an toàn khi có sự cố được các kĩ sư đường sắt xây dựng.

4.8.2 Trong giai đoạn đầu của ngành đường sắt, khái niệm an toàn khi có sự cố cố hữu đã được sử dụng. Dựa vào một tập hợp các giả thuyết, khái niệm này dựa trên việc sử dụng các bộ phận có dạng hư hỏng được xây dựng chuẩn và điều kiện an toàn tồn tại trong trường hợp hư hỏng một trong các tổng thành của nó. Tất cả những bộ phận như vậy được sắp xếp sao cho không cho phép một hệ thống được xây dựng có điều kiện vượt quá trạng thái không có hư hỏng.

4.8.3 Nói chung, tính đúng đắn của khái niệm là dựa trên kinh nghiệm nhưng bị giới hạn khả năng áp dụng đối với việc xây dựng và sử dụng các hệ thống lớn, phức tạp có sử dụng các bộ vi xử lý có trên thị trường. Sự phát triển theo cấp số mũ về số lượng các kết hợp hư hỏng được xem xét khi sử dụng những bộ phận này có nghĩa là phương pháp mang tính quyết định thường là không thể thực hiện được. Với các hệ thống phức tạp này, phương pháp mang tính xác suất có thể được sử dụng hiệu quả.

4.8.4 Phương pháp an toàn khi có sự cố có thể đúng đối với các bộ phận của một hệ thống và không bị giới hạn sử dụng bởi tiêu chuẩn này, giống như các phương pháp mang tính quyết định khác. Đối với tất cả các phương pháp, cần thiết phải đạt được sự phù hợp với các yêu cầu RAMS cụ thể đối với hệ thống.

5 Quản lý RAMS đường sắt

5.1 Yêu cầu chung

5.1.1 Mục này quy định quy trình quản lý dựa trên vòng đời hệ thống, cho phép kiểm soát các yếu tố RAMS cụ thể đối với từng hệ thống đường sắt. Quy trình sẽ hỗ trợ:

- Việc xác định các yêu cầu về RAMS;
- Đánh giá và kiểm soát các đe dọa đối với RAMS;

- Lập kế hoạch và thực hiện các nhiệm vụ RAMS;
- Các hoạt động để đạt được sự phù hợp với các yêu cầu về RAMS;
- Giám sát sự phù hợp của các hoạt động đang xảy ra trong suốt vòng đời hệ thống.

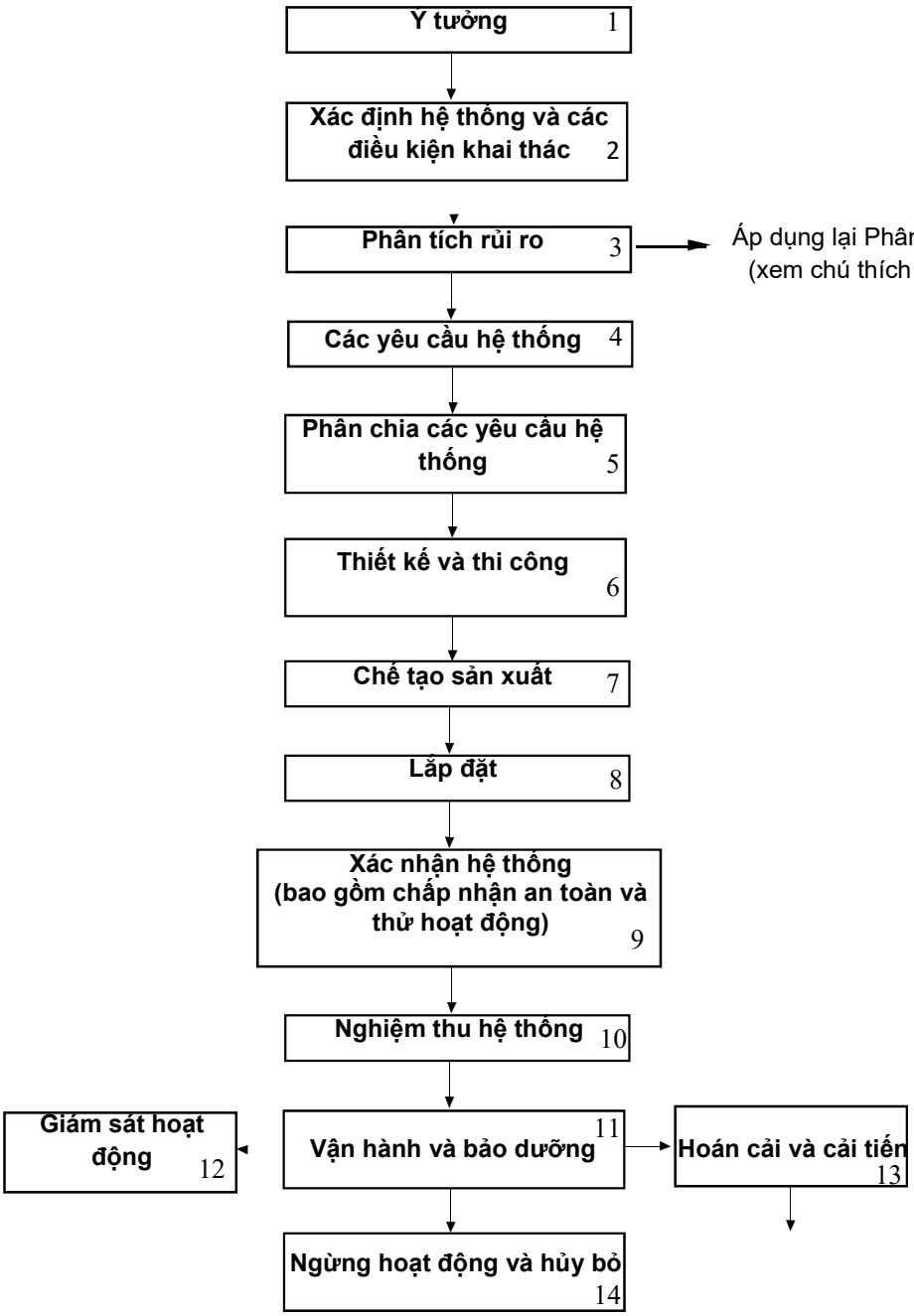
5.1.2 Mặc dù RAMS đường sắt là nội dung chính của tiêu chuẩn này, nhưng nó cũng chỉ là một trong nhiều đặc tính của toàn bộ một hệ thống đường sắt. Mục này quy định quy trình mang tính hệ thống để quản lý RAMS và là một phần trong phương pháp quản lý được tích hợp đề cập tới tất cả các mặt của hệ thống đường sắt hoàn chỉnh.

5.1.3 Rủi ro chấp nhận được về an toàn đối với hệ thống đường sắt của Doanh nghiệp đường sắt là dựa trên bộ chỉ tiêu về an toàn của Cơ quan quản lý an toàn quốc gia, hoặc của bản thân Doanh nghiệp đường sắt có sự đồng ý của Cơ quan quản lý an toàn. Trách nhiệm chính để đánh giá, kiểm soát và giảm thiểu rủi ro sẽ do Doanh nghiệp đường sắt quyết định. Trong một số trường hợp, tính pháp lý sẽ yêu cầu phải có các bằng chứng chính thức để chứng minh sự phù hợp của an toàn hệ thống.

5.2 Vòng đời hệ thống

5.2.1 Vòng đời hệ thống là một chuỗi các giai đoạn, mỗi giai đoạn có nhiều nhiệm vụ, bao quát toàn bộ sự tồn tại của hệ thống, từ khi bắt đầu cho tới khi ngừng hoạt động và hủy bỏ. Vòng đời hệ thống sẽ thể hiện biểu đồ theo thời gian để lập kế hoạch, quản lý, kiểm soát và giám sát tất cả các mặt của hệ thống, bao gồm cả RAMS, khi hệ thống tiến hành qua các giai đoạn để bố trí đúng sản phẩm ở đúng giá trị theo đúng tiến độ thời gian đã được thỏa thuận. Khái niệm vòng đời hệ thống là cơ sở cho việc thực hiện thành công tiêu chuẩn này.

5.2.2 Vòng đời hệ thống được thể hiện trong Hình 8, phù hợp với phạm vi của hệ thống đường sắt. Đối với mỗi giai đoạn của vòng đời hệ thống, các nhiệm vụ chính được tổng hợp lại trong Hình 9. Hình này sẽ thể hiện các nhiệm vụ RAMS như là các thành phần trong nhiệm vụ dự án chung. Các nhiệm vụ chung sẽ nằm ngoài phạm vi tiêu chuẩn này. Các nhiệm vụ RAMS tham gia vào các nhiệm vụ dự án chung đối với từng giai đoạn và các yêu cầu đối với nhiệm vụ RAMS sẽ được nêu chi tiết trong các mục của tiêu chuẩn này.



CHÚ THÍCH 1: Giai đoạn có thay đổi trong vòng đời hệ thống sẽ dựa trên cả hệ thống đang được thay đổi và thay đổi cụ thể được xem xét

CHÚ THÍCH 2: Phân tích rủi ro có thể được lặp lại ở một vài giai đoạn của vòng đời hệ thống (xem 6.3.1 d))

Hình 8 – Vòng đời hệ thống

Bảng 9 - Các nhiệm vụ trong giai đoạn của dự án

Giai đoạn vòng đời hệ thống	Các nhiệm vụ chung liên quan trong giai đoạn	Các nhiệm vụ RAMS liên quan trong giai đoạn	Các nhiệm vụ an toàn liên quan trong giai đoạn
1. Khái niệm	• Thiết lập phạm vi và mục đích của dự án đường sắt • Xác định ý tưởng dự án đường sắt • Tiến hành các nghiên cứu khả thi và phân tích tài chính • Thiết lập sự quản lý	• Xem xét lại việc thực hiện RAM đạt được trước đây • Xem xét các khả năng đánh giá RAM của dự án	• Xem xét sự hoạt động an toàn thu được trước đây • Xem xét các tiềm ẩn về an toàn của dự án • Xem xét chính sách và mục tiêu về an toàn
2. Xác định hệ thống và điều kiện khai thác	• Thiết lập Nhiệm vụ sơ bộ của hệ thống • Chuẩn bị Tài liệu mô tả hệ thống • Xác định chiến lược vận hành & bảo dưỡng • Xác định các điều kiện vận hành • Xác định các điều kiện bảo dưỡng • Xác định tầm ảnh hưởng của các liên kết về cơ sở hạ tầng hiện tại	• Đánh giá Dữ liệu kinh nghiệm trước đây đối với RAM • Tiến hành phân tích RAM sơ bộ • Lập chính sách về RAM • Xác định các điều kiện bảo dưỡng và vận hành dài hạn • Xác định tầm ảnh hưởng lên RAM của các liên kết với cơ sở hạ tầng hiện tại	• Đánh giá Dữ liệu kinh nghiệm trước đây về an toàn • Tiến hành Phân tích Nguy hiểm sơ bộ • Thiết lập Kế hoạch an toàn (toàn bộ) • Xác định Mức cho phép đối với các chỉ tiêu rủi ro • Xác định phạm vi ảnh hưởng lên an toàn của các liên kết với cơ sở hạ tầng hiện tại
3. Phân tích rủi ro (xem chú ý 6)	• Tiến hành phân tích rủi ro liên quan tới dự án		• Tiến hành phân tích nguy hiểm hệ thống và rủi ro về an toàn • Lập Sổ tay nguy hiểm • Tiến hành Đánh giá rủi ro
4. Các yêu cầu hệ thống	• Tiến hành phân tích các yêu cầu • Quy định hệ thống (Các yêu cầu tổng hợp) • Quy định về môi trường • Quy định Thuyết minh hệ thống & Chỉ tiêu chấp nhận (các yêu cầu tổng hợp)	• Quy định các yêu cầu về RAM cho hệ thống (tổng hợp) • Xác định chỉ tiêu chấp nhận RAM (tổng hợp) • Xác định Cấu trúc chức năng hệ thống • Thiết lập Chương trình RAM	• Quy định các yêu cầu về an toàn của hệ thống (tổng hợp) • Xác định chỉ tiêu chấp nhận về an toàn (tổng hợp)

Bảng 9 – Các nhiệm vụ trong giai đoạn của dự án (tiếp theo)

Giai đoạn vòng đời hệ thống	Các nhiệm vụ chung liên quan trong giai đoạn	Các nhiệm vụ RAMS liên quan trong giai đoạn	Các nhiệm vụ an toàn liên quan trong giai đoạn
	• Thiết lập Kế hoạch xác nhận • Thiết lập Các yêu cầu về quản lý, chất lượng và tổ chức • Thực hiện quy trình kiểm soát sự thay đổi	• Thiết lập Quản lý RAM	• Xác định các yêu cầu chức năng liên quan tới an toàn • Thiết lập Quản lý về an toàn
5. Phân chia các yêu cầu của hệ thống	• Phân chia các yêu cầu của hệ thống - Quy định các yêu cầu cho hệ thống con & các tổng thành - Xác định chỉ tiêu chấp nhận cho hệ thống con và các tổng thành	• Phân chia các yêu cầu về RAM của hệ thống - Quy định các yêu cầu về RAM cho hệ thống con và tổng thành - Xác định chỉ tiêu chấp nhận RAM cho hệ thống con và các tổng thành	• Phân chia các yêu cầu và mục tiêu về an toàn của hệ thống - Quy định các yêu cầu về an toàn cho hệ thống con và các tổng thành - Xác định chỉ tiêu chấp nhận về an toàn của hệ thống con và các tổng thành • Cập nhật Kế hoạch an toàn hệ thống
6. Thiết kế và thi công	• Tiến hành lập kế hoạch • Tiến hành thiết kế và xây dựng • Tiến hành phân tích và thử nghiệm thiết kế • Tiến hành thẩm tra thiết kế • Tiến hành Thi công và Thẩm định • Tiến hành Thiết kế các nguồn lực cung ứng	• Thực hiện Chương trình RAM bằng Xem xét, phân tích, thử nghiệm và đánh giá dữ liệu, đối với: - Độ tin cậy và tính sẵn sàng - Hoạt động bảo dưỡng và khả năng bảo dưỡng - Chính sách bảo dưỡng tối ưu - Nguồn lực cung ứng • Tiến hành Kiểm soát chương trình, đối với: - Quản lý chương trình RAM - Kiểm soát các nhà thầu phụ và bên cung ứng	Thực hiện Kế hoạch an toàn bằng xem xét, phân tích, thử nghiệm và đánh giá dữ liệu, đối với: • Sổ tay nguy hiểm • Phân tích nguy hiểm và Đánh giá rủi ro • Đánh giá cơ sở quyết định thiết kế liên quan tới an toàn • Thực hiện Kiểm soát chương trình, đối với: - Quản lý an toàn - Kiểm soát các nhà thầu phụ và bên cung ứng • Chuẩn bị Hồ sơ an toàn chung

Bảng 9 – Các nhiệm vụ trong giai đoạn của dự án (tiếp theo)

Giai đoạn vòng đời hệ thống	Các nhiệm vụ chung liên quan trong giai đoạn	Các nhiệm vụ RAMS liên quan trong giai đoạn	Các nhiệm vụ an toàn liên quan trong giai đoạn
			• Chuẩn bị Hồ sơ an toàn khai thác chung (nếu phù hợp)
7. Chế tạo sản xuất	• Tiến hành Lập kế hoạch sản xuất • Chế tạo • Chế tạo và Thử nghiệm việc lắp ráp phụ các bộ phận • Chuẩn bị cho việc lưu trữ hồ sơ • Thiết lập quá trình đào tạo	• Tiến hành xem xét các tác động về môi trường • Tiến hành Thử nghiệm cải tiến RAM • Triển khai Báo cáo hư hỏng và hệ thống hoạt động sửa chữa (FRACAS)	• Thực hiện Kế hoạch an toàn bằng: xem xét, phân tích, Thử nghiệm và đánh giá dữ liệu • Sử dụng Sổ tay nguy hiểm
8. Lắp đặt	• Lắp ráp hệ thống • Lắp đặt hệ thống	• Triển khai đào tạo nhân lực bảo trì hệ thống • Thiết lập sự dự phòng cho các bộ phận và dụng cụ	• Thiết lập chương trình lắp đặt • Thực hiện chương trình lắp đặt
9. Xác nhận hệ thống (bao gồm chấp nhận an toàn và thử hoạt động)	• Thử hoạt động • Thực hiện Thời kì vận hành thử • Thực hiện việc đào tạo	• Tiến hành Chứng minh RAM	• Thiết lập Chương trình thử hoạt động • Thực hiện Chương trình thử hoạt động • Chuẩn bị Hồ sơ an toàn ứng dụng cụ thể
10.Chấp nhận hệ thống	• Tiến hành các quy trình chấp nhận, dựa trên chỉ tiêu chấp nhận • Thu thập bằng chứng để chấp nhận • Đưa vào khai thác • Tiếp tục Thời kì vận hành thử thách (nếu phù hợp)	• Đánh giá chứng minh RAM	• Đánh giá Hồ sơ an toàn ứng dụng cụ thể
11.Vận hành và bảo dưỡng	• Vận hành hệ thống dài hạn • Tiến hành duy trì bảo dưỡng • Thực hiện duy trì đào tạo	• Duy trì cung ứng các phụ tùng thay thế và dụng cụ	• Tiến hành duy trì bảo dưỡng lấy độ tin cậy làm trung tâm

Giai đoạn vòng đời hệ thống	Các nhiệm vụ chung liên quan trong giai đoạn	Các nhiệm vụ RAMS liên quan trong giai đoạn	Các nhiệm vụ an toàn liên quan trong giai đoạn
		• Tiến hành duy trì bảo dưỡng, nguồn lực cung ứng lấy độ tin cậy làm trung tâm	• Tiến hành duy trì giám sát hoạt động an toàn và duy trì Sổ tay nguy hiểm
12.Giám sát hoạt động	• Thu thập các thống kê hoạt động vận hành • Thu thập, phân tích và đánh giá dữ liệu	• Thu thập, phân tích, đánh giá và sử dụng thống kê hoạt động và RAM	• Thu thập, phân tích, đánh giá sử dụng các thống kê về hoạt động và an toàn
13.Thay đổi và cải tiến	• Thực hiện các quy trình yêu cầu thay đổi • Thực hiện các quy trình thay đổi và cải tiến	• Xem xét các khả năng về RAM đối với thay đổi và cải tiến	• Xem xét các khả năng về an toàn đối với thay đổi và cải tiến
14.Ngừng hoạt động và hủy bỏ	• Lập kế hoạch ngừng hoạt động và hủy bỏ • Tiến hành ngừng hoạt động • Tiến hành hủy bỏ	• Không có hoạt động cho RAM	• Thiết lập Kế hoạch an toàn • Tiến hành phân tích rủi ro và đánh giá rủi ro • Thực hiện Kế hoạch an toàn

CHÚ THÍCH 1: Hoạt động kiểm soát thay đổi và quản lý cấu hình áp dụng cho tất cả các giai đoạn của dự án

CHÚ THÍCH 2: Các hoạt động thẩm tra và xác nhận áp dụng trong hầu hết các giai đoạn vòng đời hệ thống và nằm trong nội dung chính

CHÚ THÍCH 3: Đối với RAM, thuật ngữ "Chương trình RAM" được sử dụng phổ biến và được thay đổi cho phù hợp với tiêu chuẩn này. Đối với an toàn, thuật ngữ "Kế hoạch an toàn" được sử dụng phổ biến và được thay đổi phù hợp cho tiêu chuẩn này

CHÚ THÍCH 4: Chú ý phạm vi của tiêu chuẩn này bị giới hạn trong RAMS và không đề cập tới tất cả các hoạt động bảo đảm hệ thống. Tuy nhiên, cần thiết đảm bảo việc đồng bộ giữa các giai đoạn RAMS và các giai đoạn liên quan tới dự án và để thỏa thuận các điều kiện cần thiết từ giai đoạn này sang giai đoạn khác, theo quan điểm về RAMS.

CHÚ THÍCH 5: Các hoạt động trong giai đoạn 9 và 10 có thể được tích hợp, dựa trên hệ thống đường sắt được xem xét

CHÚ THÍCH 6: Phân tích rủi ro có thể được lặp lại ở một số giai đoạn (xem mục 4.6.2 và 6.3.1 d))

5.2.3 Tiêu chuẩn này thừa nhận sự cân đối giữa đặc tính RAMS của một hệ thống và chi phí xây dựng và sở hữu hệ thống, được biết tới như chi phí vòng đời hệ thống. Tiêu chuẩn này yêu cầu việc xem xét các chi phí vòng đời hệ thống kết hợp với các vấn đề RAMS của hệ thống. Tuy nhiên, sẽ không đưa ra các giải pháp đối với các vấn đề về RAMS dựa trên cơ sở về chi phí, khi đây là trách nhiệm của Doanh nghiệp đường sắt.

5.2.4 Điều 6 và các mục trong điều 6 sẽ quy định các mục tiêu, các yêu cầu, các đầu vào và các tài liệu chuyển giao trong các nhiệm vụ RAMS theo một phương thức thống nhất đối với từng giai đoạn trong vòng đời hệ thống và trong phạm vi của toàn bộ một dự án,.

5.2.5 Quy trình sẽ hỗ trợ cho quá trình cung ứng bằng việc đưa ra một loạt các nhiệm vụ tổng hợp trong các giai đoạn vòng đời hệ thống. Điều này là cơ sở cho các cam kết chính thức đối với riêng từng nhiệm vụ RAMS hoặc cho việc kết hợp các nhiệm vụ có trong một quy trình quản lý tích hợp. Trách nhiệm cho việc thực hiện các nhiệm vụ sẽ dựa trên hệ thống được xem xét và các điều kiện có thể áp dụng của hợp đồng. Một số hướng dẫn chung cho việc thiết lập các trách nhiệm này được đưa ra trong Phụ lục E.

5.2.6 Tiêu chuẩn này trình bày vòng đời hệ thống theo thứ tự, thể hiện riêng từng giai đoạn và các mối liên kết giữa các giai đoạn. Các kiểu thể hiện vòng đời hệ thống khác sẽ được mở rộng trong ngành công nghiệp và bao gồm cả kiểu chữ “V”.

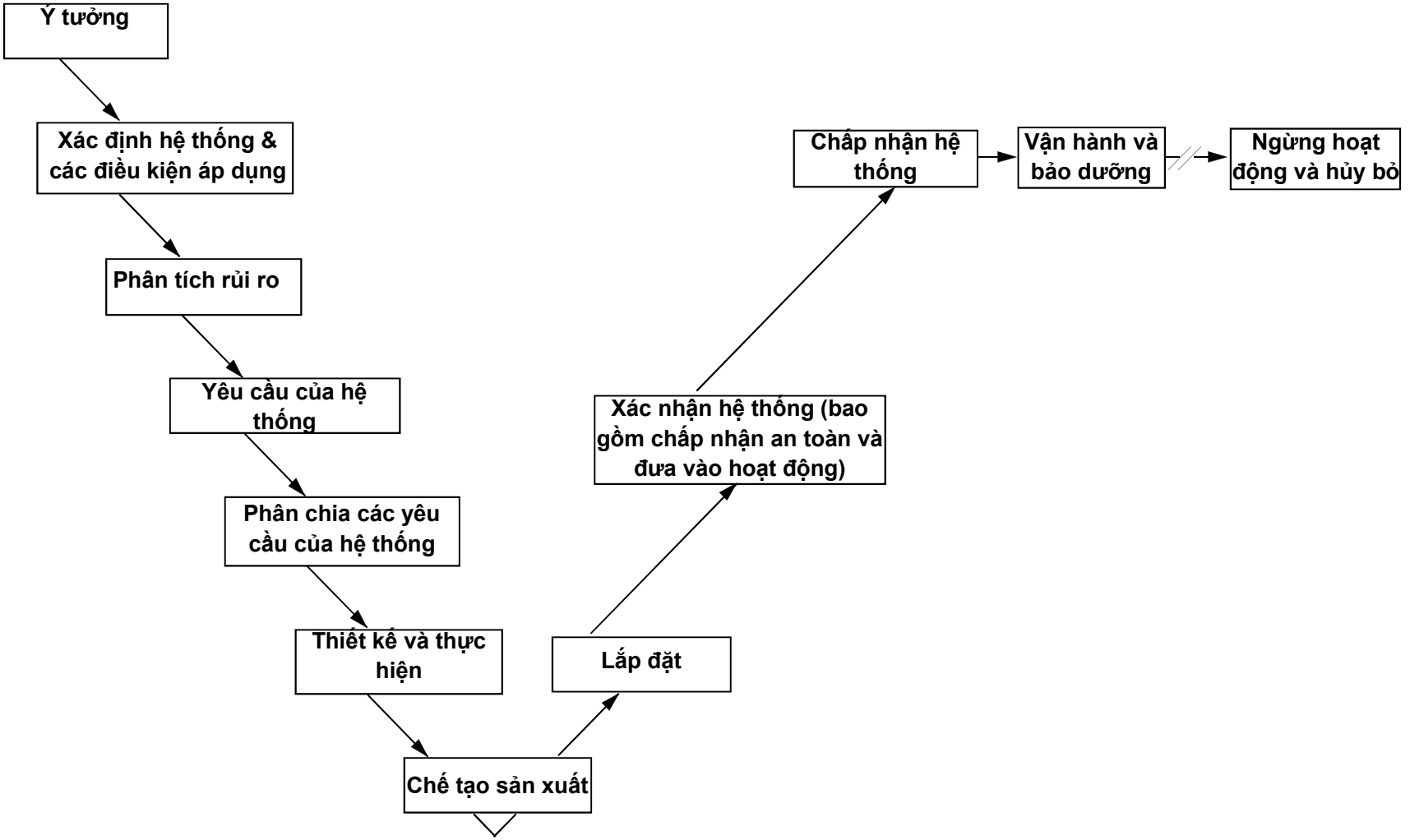
5.2.7 Hình 10 trình bày một dạng thể hiện vòng đời hệ thống theo kiểu chữ “V” có trong tiêu chuẩn này. Nhánh từ trên xuống (bên trái) thường được gọi là quá trình xây dựng và là một quá trình cải tiến, kết thúc bằng quá trình sản xuất các tổng thành của hệ thống. Nhánh từ dưới lên (bên phải) liên quan tới việc lắp ráp, lắp đặt, chuyển giao và sau đó là quá trình vận hành toàn bộ hệ thống.

5.2.8 Cách thể hiện chữ “V” giả thiết các hoạt động của quá trình chấp nhận sẽ liên kết về mặt bản chất với các hoạt động xây dựng khi những hoạt động được thiết kế thực tế phải được kiểm tra lần cuối theo các yêu cầu. Do vậy, các hoạt động xác nhận cho việc chấp nhận ở các giai đoạn khác nhau của hệ thống sẽ dựa trên quy định chỉ dẫn kĩ thuật hệ thống và nên được lập kế hoạch ở các giai đoạn trước đó, ví dụ: bắt đầu ở các giai đoạn xây dựng tương ứng của vòng đời hệ thống. Liên kết như vậy được thể hiện trong Hình 11.

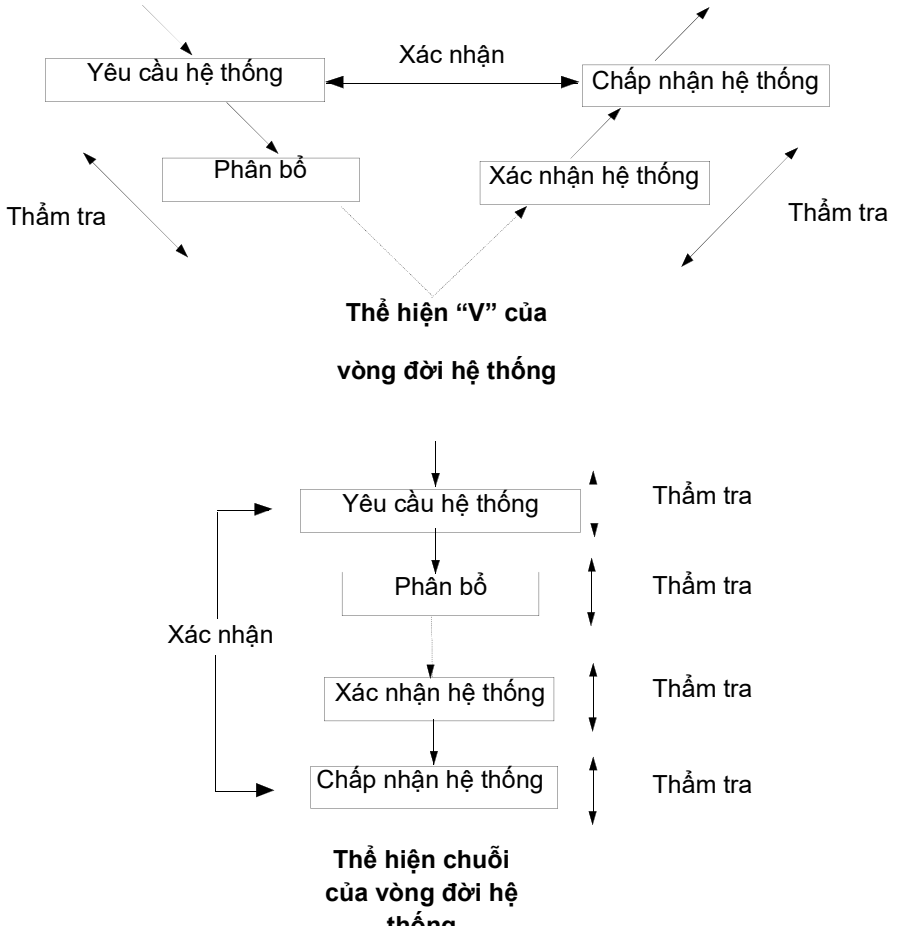
5.2.9 Việc thể hiện theo cách chữ V này là hiệu quả trong việc đưa ra các nhiệm vụ xác nhận và thẩm tra trong vòng đời hệ thống. Mục đích của việc thẩm tra là để chứng minh xem, đối với các đầu vào cụ thể, các tài liệu chuyển giao của mỗi giai đoạn có đáp ứng tất cả các yêu cầu của giai đoạn đó. Mục đích của việc xác nhận là để chứng minh xem hệ thống được xem xét có đáp ứng các yêu cầu của nó theo tất cả các mặt ở bất kì giai đoạn nào trong quá trình xây dựng và sau khi lắp đặt.

5.2.10 Trong tiêu chuẩn này, các nhiệm vụ thẩm tra sẽ nằm trong mỗi giai đoạn vòng đời hệ thống. Mặc dù tiêu chuẩn này liên quan tới việc đảm bảo hệ thống theo các nội dung về RAMS, nhưng các

nhiệm vụ thẩm tra và xác nhận (V&V) sẽ là không thể thiếu trong việc chứng minh một cách toàn diện việc đảm bảo các hệ thống. Do đó, V&V RAMS sẽ góp phần vào V&V đảm bảo toàn bộ hệ thống.



Hình 10 – Sơ đồ chữ "V" thể hiện vòng đời hệ thống



CHÚ THÍCH: mục 5.2.9 đưa ra thông tin thêm về vai trò của thẩm tra và xác nhận

Hình 11 – Thẩm tra và xác nhận

5.3 Áp dụng tiêu chuẩn

5.3.1 Mục này đưa ra các yêu cầu cho việc thực hiện một cách linh hoạt và hiệu quả tiêu chuẩn này đối với các hệ thống đường sắt, về mặt quy mô, độ phức tạp và chi phí.

5.3.2 Các yêu cầu được quy định trong tiêu chuẩn này là phổ biến và có khả năng áp dụng cho tất cả các loại hình của hệ thống đường sắt. Doanh nghiệp đường sắt phải quy định việc áp dụng các yêu cầu của tiêu chuẩn này cho hệ thống được xem xét. Việc đánh giá phải dựa trên khả năng áp dụng của các yêu cầu đối với riêng từng hệ thống. Sẽ yêu cầu chú ý cụ thể trong quá trình đánh giá chuỗi các nhiệm vụ được tiến hành trong giai đoạn 9 - Xác nhận hệ thống và giai đoạn 10 – Chấp nhận hệ thống.

5.3.3 Trong các trường hợp hoán cải hệ thống, thường có một giai đoạn "giai đoạn hỗn hợp" khi các quá trình vận hành các hệ thống hiện có và hệ thống mới sẽ kết hợp với nhau, hoặc được vận hành tại cùng một thời điểm. Trong các trường hợp như vậy, các nghiên cứu về an toàn phải đề cập cụ thể tới các tác động có thể của quá trình tương tác giữa các hệ thống hiện có và hệ thống được hoán cải.

5.3.4 Việc áp dụng tiêu chuẩn này phải được thay đổi phù hợp với các yêu cầu cụ thể của hệ thống được xem xét. Việc đánh giá khả năng áp dụng tiêu chuẩn này đối với hệ thống được xem xét phải:

a) Quy định các giai đoạn vòng đời hệ thống được yêu cầu để xác định hệ thống được xem xét, đưa ra các lý do cho từng giai đoạn vòng đời hệ thống được quy định và chứng minh các nhiệm vụ được tiến hành trong những giai đoạn vòng đời hệ thống này thỏa mãn các nguyên tắc của các yêu cầu trong tiêu chuẩn này.

b) Quy định các hoạt động bắt buộc và các yêu cầu của từng giai đoạn vòng đời hệ thống cần thiết, có sử dụng Hình 9 và các thông tin liên quan đến giai đoạn tương ứng trong điều 6 như một danh sách kiểm tra, bao gồm:

- Phạm vi của mỗi yêu cầu có liên quan tới hệ thống được xem xét;

- Các phương pháp, các công cụ và các kĩ thuật cần thiết dựa trên mỗi yêu cầu, phạm vi và mức độ áp dụng chúng;

- Các hoạt động thẩm tra và xác nhận cần thiết dựa trên từng yêu cầu và phạm vi áp dụng chúng;

- Tất cả tài liệu hỗ trợ.

c) Xác minh mọi sự khác biệt so với các hoạt động và các yêu cầu trong tiêu chuẩn này.

d) Xác minh sự phù hợp của các nhiệm vụ được lựa chọn đối với hệ thống được xem xét.

5.3.5 Trong mọi áp dụng tiêu chuẩn này, các yêu cầu dưới đây là bắt buộc:

a) Trách nhiệm để thực hiện tất cả các nhiệm vụ về RAMS trong mỗi giai đoạn của vòng đời hệ thống phải được quy định và được đồng ý cho hệ thống được xem xét, bao gồm cả sự tương giao giữa các nhiệm vụ liên quan.

b) Tất cả các cá nhân có trách nhiệm trong quy trình quản lý RAMS phải đủ năng lực để thực hiện các trách nhiệm này.

c) Việc thiết lập và thực hiện Chương trình RAM và Kế hoạch an toàn sẽ là các nội dung chính trong việc xác định các hệ thống đáng tin cậy. Khi nội dung của những tài liệu được lên kế hoạch này được cụ thể cho hệ thống được xem xét, nhiều nhiệm vụ RAMS sẽ yêu cầu các hoạt động phân tích giống nhau. Tuy nhiên, các liên kết ràng buộc đối với những hoạt động này có thể khác nhau. Đối với các nhiệm vụ tập trung vào RAM, các xem xét về chi phí có khả năng sẽ là công việc chính dẫn đường, trong khi đối với các nhiệm vụ tập trung vào an toàn, lại là xem xét về việc tránh tai nạn và các sự cố. Trong trường hợp này, các yêu cầu về RAMS có thể xung đột, khi các hậu quả về kinh tế trong RAMS có thể khác nhau, phụ thuộc vào các yêu cầu của Doanh nghiệp đường sắt. Việc xác định yêu cầu cho

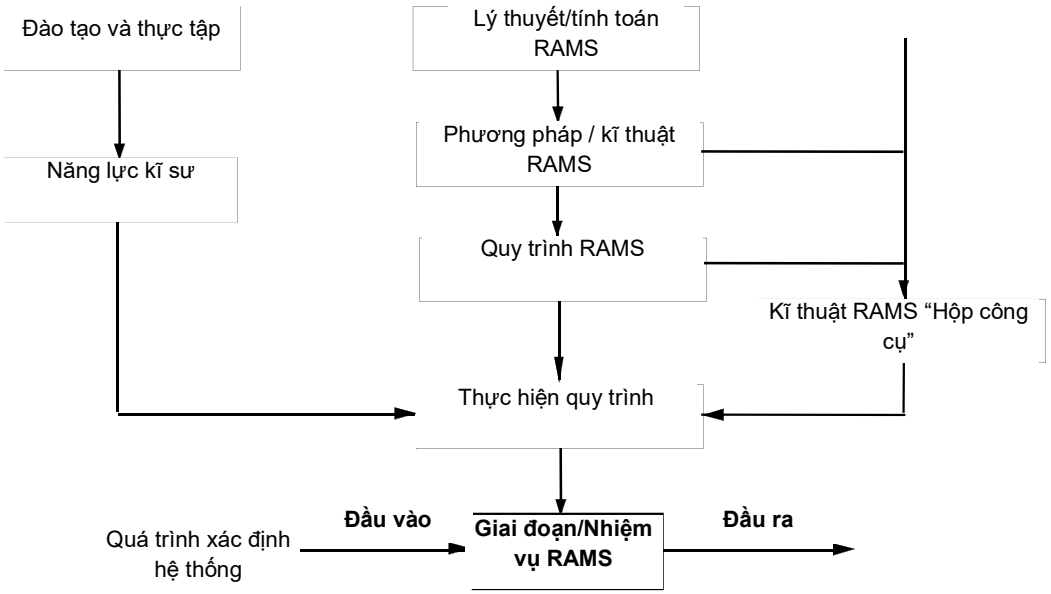
việc quy định và quản lý các xung đột về RAMS phải có trong các tài liệu lập kế hoạch RAMS, cùng với mọi chi tiết của tất cả các phân tích RAMS, khi mà mức độ của các hoạt động phân tích có thể khác nhau giữa các nhiệm vụ RAMS.

d) Các yêu cầu của tiêu chuẩn này phải được thực hiện trong các quá trình kinh doanh, được hỗ trợ bởi Hệ thống quản lý chất lượng (QMS) thỏa mãn các yêu cầu của EN ISO 9001, EN ISO 9002 hoặc EN ISO 9003 phù hợp với hệ thống được xem xét.

e) Một hệ thống quản lý cấu hình phù hợp và hiệu quả phải được thiết lập và thực hiện, đề cập tới các nhiệm vụ RAMS trong tất cả các giai đoạn vòng đời hệ thống. Phạm vi của quá trình quản lý cấu hình sẽ dựa trên hệ thống được xem xét, nhưng thông thường phải bao gồm tất cả các dữ liệu hệ thống và tất cả các tài liệu chuyển giao hệ thống khác.

5.3.6 Điều 6 này mô tả chi tiết các phương pháp để đảm bảo việc đạt được các yêu cầu về RAMS thông qua việc giảm thiểu các tác động của mọi sự hư hại và kiểm soát các yếu tố được nêu trong điều 4, thông qua việc quy định quy trình quản lý dựa trên vòng đời hệ thống. Các phương pháp, các công cụ và các kĩ thuật phù hợp với các hệ thống tin cậy về mặt kĩ thuật được trình bày trong các tiêu chuẩn khác (xem Phụ lục B). Chú ý việc lựa chọn các phương pháp, công cụ và kĩ thuật, mức độ áp dụng và phạm vi áp dụng của việc ứng dụng chúng và của các tài liệu phải được tương xứng với các yêu cầu của hệ thống được xem xét. Điều này nên được thỏa thuận giữa Doanh nghiệp đường sắt và đơn vị cung ứng cho hệ thống được xem xét. Hình 12 thể hiện một cách nhìn tổng quát về cách thức những vấn đề khác nhau này liên quan tới việc hỗ trợ kĩ thuật và quản lý RAMS.

5.3.7 Các yêu cầu nêu chi tiết trong tiêu chuẩn này được sử dụng để hỗ trợ quá trình đánh giá (audit). Doanh nghiệp đường sắt và đơn vị công nghiệp phụ trợ đường sắt đối với hệ thống được xem xét phải đồng ý và thực hiện Kế hoạch đánh giá (Audit Plan) đề cập tới việc áp dụng các yêu cầu của tiêu chuẩn này, khi được thay đổi cho phù hợp với hệ thống.



Hình 12 – Kĩ thuật và quản lý RAMS được thực hiện trong quá trình xác định hệ thống

6 Vòng đời hệ thống RAMS

Điều 6 này nêu chi tiết các mục tiêu, các yêu cầu, các tài liệu chuyển giao và các hoạt động thẩm tra và xác nhận được tiến hành trong suốt các giai đoạn vòng đời hệ thống. Phạm vi và cách áp dụng các yêu cầu phải được đánh giá và được thay đổi cho phù hợp để đáp ứng các yêu cầu cụ thể của hệ thống được xem xét. Để bổ sung thêm thông tin về điều 6 này, xem mục 5.3 trong tiêu chuẩn này.

6.1 Giai đoạn 1: Khái niệm

6.1.1 Mục tiêu

Mục tiêu của giai đoạn này là phải xây dựng một mức độ hiểu biết hệ thống đủ để đảm bảo tất cả các nhiệm vụ vòng đời hệ thống RAMS sau đó được thực hiện một cách hợp lý.

6.1.2 Các đầu vào

Đầu vào cho giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng các yêu cầu của giai đoạn, ví dụ: các tuyên bố về phạm vi và mục đích cho dự án.

6.1.3 Các yêu cầu

6.1.3.1 Yêu cầu 1 của giai đoạn này là phải thu thập sự hiểu biết về nội dung đặc tính về RAMS đối với:

a) Phạm vi, nội dung và mục đích của hệ thống.

b) Môi trường của hệ thống, bao gồm:

- Các vấn đề về vật lý;
- Các vấn đề tiềm ẩn chung của hệ thống;
- Các vấn đề về xã hội;
- Các vấn đề về chính trị;
- Các vấn đề về pháp lý;
- Các vấn đề về kinh tế.

c) Các yếu tố tiềm ẩn chung liên quan đến RAMS của hệ thống.

6.1.3.2 Yêu cầu 2 của giai đoạn này là phải xem xét:

a) Các yếu tố tiềm ẩn liên quan đến RAMS trong mọi phân tích tài chính của hệ thống.

b) Các yếu tố tiềm ẩn liên quan đến RAMS trong mọi nghiên cứu khả thi hệ thống.

6.1.3.3 Yêu cầu 3 của giai đoạn này là phải xác định các nguồn gây nguy hiểm mà có thể ảnh hưởng tới đặc tính RAMS của hệ thống, bao gồm:

- Sự tương tác với các hệ thống khác;
- Sự tương tác với con người;

6.1.3.4 Yêu cầu 4 của giai đoạn này là phải thu được thông tin về:

a) Các yêu cầu về RAMS trước đó và các đặc tính RAMS trước đây của các hệ thống tương tự và/hoặc có liên quan.

b) Các nguồn gây nguy hiểm đã được xác định đối với đặc tính RAMS.

c) Chính sách an toàn hiện tại của doanh nghiệp đường sắt và các mục tiêu.

d) Quy định pháp lý về an toàn.

6.1.3.5 Yêu cầu 5 của giai đoạn này là phải xác định phạm vi của các yêu cầu quản lý đối với các nhiệm vụ RAMS tiếp theo trong vòng đời hệ thống.

6.1.4 Tài liệu chuyển giao

6.1.4.1 Các kết quả từ giai đoạn này phải được ghi lại, cùng với các giả thiết và các minh chứng đưa ra trong suốt giai đoạn.

6.1.4.2 Các tài liệu chuyển giao phải có cấu trúc về quản lý phù hợp để thực hiện các yêu cầu về RAMS trong các giai đoạn vòng đời hệ thống 2, 3 & 4.

6.1.4.3 Các tài liệu chuyển giao từ giai đoạn này là đầu vào chủ yếu cho các giai đoạn vòng đời hệ thống tiếp theo.

6.1.5 Thẩm tra

Các nhiệm vụ thẩm tra dưới đây phải được tiến hành trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi cần là các dữ liệu và các số liệu thống kê khác, được sử dụng làm đầu vào của các nhiệm vụ RAMS trong giai đoạn này.

b) Đánh giá khả năng phù hợp của tuyên bố về môi trường hệ thống được xác định theo yêu cầu 1.

c) Đánh giá mức độ hoàn chỉnh của quá trình liệt kê các nguồn gây nguy hiểm được xác định theo yêu cầu 3.

d) Đánh giá sự phù hợp của các phương pháp, công cụ và kĩ thuật được sử dụng trong giai đoạn.

e) Đánh giá năng lực của toàn bộ nhân lực thực hiện các nhiệm vụ trong giai đoạn.

6.2 Giai đoạn 2: Xác định hệ thống và các điều kiện áp dụng

6.2.1 Mục tiêu

Mục tiêu của giai đoạn này là để:

a) Xác định hồ sơ nhiệm vụ của hệ thống.

b) Xác định giới hạn của hệ thống.

c) Thiết lập các điều kiện áp dụng ảnh hưởng tới các đặc tính kĩ thuật của hệ thống.

d) Xác định phạm vi của phân tích nguy hiểm hệ thống.

e) Thiết lập chính sách về RAMS cho hệ thống.

f) Thiết lập Kế hoạch an toàn cho hệ thống.

Do các vấn đề này ảnh hưởng tới đặc tính RAMS tiềm ẩn của hệ thống.

6.2.2 Đầu vào

Đầu vào cho giai đoạn này phải bao gồm các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng các yêu cầu của giai đoạn, bao gồm các tài liệu chuyển giao của giai đoạn 1.

6.2.3 Các yêu cầu

6.2.3.1 Yêu cầu 1 của giai đoạn này là phải xác định:

a) Hồ sơ nhiệm vụ hệ thống, bao gồm:

- Các yêu cầu về hoạt động;
- Các mục tiêu về RAMS;
- Chiến lược và điều kiện vận hành dài hạn;
- Chiến lược và điều kiện bảo dưỡng dài hạn;
- Các xem xét tuổi thọ hệ thống, bao gồm các vấn đề về chi phí vòng đời hệ thống;
- Xem xét các yếu tố cung ứng.

b) Giới hạn hệ thống, bao gồm:

- Các tương giao với môi trường vật lý;
- Các tương giao với các hệ thống công nghệ khác;
- Các tương giao với con người;
- Mối quan hệ với các doanh nghiệp đường sắt.

c) Phạm vi của các điều kiện áp dụng ảnh hưởng tới hệ thống, bao gồm:

- Các liên kết ràng buộc phát sinh bởi các cơ sở hạ tầng hiện có;
- Các điều kiện vận hành hệ thống;
- Các điều kiện bảo dưỡng hệ thống;
- Các xem xét về nguồn lực cung ứng;
- Xem xét các thông tin kinh nghiệm trước đây của các hệ thống tương đương.

d) Phạm vi của phân tích nguy hiểm hệ thống, bao gồm việc xác định:

- Các nguy hiểm có sẵn trong quy trình được kiểm soát;

- Các nguy hiểm về môi trường;
- Các nguy hiểm về an ninh;
- Ảnh hưởng của các tình huống bên ngoài;
- Các giới hạn của hệ thống được phân tích;
- Ảnh hưởng của các liên kết ràng buộc với cơ sở hạ tầng hiện có lên RAMS;

6.2.3.2 Yêu cầu 2 của giai đoạn này là phải thực hiện:

a) Phân tích RAM sơ bộ để hỗ trợ các mục tiêu.

b) Xác định nguy hiểm sơ bộ để:

- Xác định các hệ thống con liên quan tới các nguy hiểm đã biết;
- Xác định các kiểu tình huống dẫn đến tai nạn mà cần được xem xét, bao gồm các hư hỏng tổng thành, các lỗi về quy trình, lỗi con người và các cơ chế hư hỏng phụ thuộc.
- Xác định chỉ tiêu chấp nhận rủi ro ban đầu.

6.2.3.3 Yêu cầu 3 của giai đoạn này là phải thiết lập ra chính sách chung về RAMS cho hệ thống, bao gồm các yêu cầu về khái niệm an toàn và chính sách của Doanh nghiệp đường sắt đối với việc giải quyết mọi xung đột phát sinh giữa “tính sẵn sàng” và “độ an toàn”.

6.2.3.4 Yêu cầu 4 của giai đoạn này là phải thiết lập Kế hoạch an toàn cho hệ thống. Kế hoạch an toàn phải được doanh nghiệp đường sắt và đơn vị công nghiệp phụ trợ đường sắt đồng ý đối với hệ thống được xem xét và phải được thực hiện, xem xét và duy trì trong suốt vòng đời hệ thống của hệ thống. Kế hoạch an toàn nên có:

a) Chính sách và chiến lược để đạt được sự an toàn.

b) Phạm vi của kế hoạch.

c) Mô tả về hệ thống.

d) Chi tiết về các vai trò, các trách nhiệm, năng lực và mối quan hệ của các tổ chức tiến hành các nhiệm vụ có trong vòng đời hệ thống.

e) Mô tả về vòng đời hệ thống và các nhiệm vụ an toàn được thực hiện trong vòng đời hệ thống cùng với bất kì sự phụ thuộc nào.

f) Các quy trình kĩ thuật, phân tích và đánh giá an toàn được áp dụng trong suốt vòng đời hệ thống, bao gồm các quy trình:

- Đảm bảo mức độ độc lập phù hợp của các cá nhân khi thực hiện nhiệm vụ, tương xứng với rủi ro của hệ thống;
- Nhận biết và phân tích nguy hiểm;
- Đánh giá rủi ro và quản lý rủi ro hiện có;
- Xây dựng chỉ tiêu chấp nhận rủi ro;
- Thiết lập và xem xét sự phù hợp hiện có của các yêu cầu an toàn;
- Thiết kế hệ thống;
- Thẩm tra và xác nhận;
- Đánh giá an toàn, để đạt được sự phù hợp giữa các yêu cầu và xác định hệ thống;
- Kiểm toán an toàn, để đạt được sự phù hợp của quy trình quản lý với kế hoạch an toàn;
- Đánh giá an toàn để đạt được sự phù hợp giữa phân tích an toàn hệ thống con và hệ thống.

g) Chi tiết của các tài liệu chuyển giao liên quan tới an toàn trong vòng đời hệ thống, bao gồm:

- Hồ sơ tài liệu;
- Phần cứng;
- Phần mềm

h) Quy trình chuẩn bị Hồ sơ an toàn hệ thống.

i) Quy trình chấp thuận an toàn hệ thống.

j) Quy trình chấp thuận an toàn cho việc hoán cải hệ thống.

k) Quy trình phân tích các hoạt động vận hành và bảo dưỡng để đảm bảo độ an toàn được xác định phù hợp với các yêu cầu.

l) Quy trình duy trì hồ sơ tài liệu liên quan tới an toàn, bao gồm Sổ tay nguy hiểm (*Hazard Log*).

m) Các tương giao với các chương trình và kế hoạch liên quan khác.

n) Các ràng buộc và các giả thiết được tạo ra trong kế hoạch.

o) Bố trí quản lý nhà thầu phụ.

p) Các yêu cầu cho việc kiểm toán an toàn định kì, đánh giá an toàn và xem xét an toàn, trong suốt vòng đời hệ thống và các yêu cầu phù hợp với sự liên quan về mặt an toàn của hệ thống được xem xét, bao gồm các yêu cầu về sự độc lập của mọi cá nhân.

6.2.4 Tài liệu chuyển giao

6.2.4.1 Các kết quả của giai đoạn này phải được lưu lại, với mọi giả thiết và minh chứng được thực hiện trong suốt giai đoạn.

6.2.4.2 Các tài liệu chuyển giao phải có Chính sách về RAMS cho hệ thống.

6.2.4.3 Các tài liệu chuyển giao phải gồm Kế hoạch an toàn cho hệ thống.

6.2.4.4 Các tài liệu chuyển giao từ giai đoạn này sẽ là đầu vào chủ yếu cho các giai đoạn vòng đời hệ thống tiếp theo.

6.2.5 Thẩm tra

6.2.5.1 Các nhiệm vụ thẩm tra dưới đây phải được tiến hành trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi cần là các dữ liệu và các thống kê khác được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này.

b) Thẩm tra các vấn đề RAMS trong các tài liệu chuyển giao giai đoạn 2 với các tài liệu chuyển giao của giai đoạn 1, đặc biệt phải đánh giá Chính sách RAMS về sự phù hợp theo các yêu cầu hệ thống được quy định trong giai đoạn 1.

c) Đánh giá mức độ hoàn chỉnh của phân tích RAM và quy trình xác định nguy hiểm.

d) Đánh giá sự phù hợp của Kế hoạch an toàn, bao gồm việc xem xét sự phù hợp của mọi nguồn dữ liệu có trong Kế hoạch an toàn.

e) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn.

f) Đánh giá năng lực của tất cả cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.2.5.2 Mọi lỗi hoặc thiếu sót có thể sẽ yêu cầu áp dụng lại một số hoặc tất cả các hoạt động của một hoặc tất cả các giai đoạn vòng đời hệ thống trước đó.

6.3 Giai đoạn 3: phân tích rủi ro

CHÚ THÍCH: Phân tích rủi ro có thể cần được lặp lại tại một số giai đoạn của vòng đời hệ thống (xem mục d của 6.3.1 dưới đây)

6.3.1 Mục tiêu

Mục tiêu của giai đoạn này là để:

a) Xác định các nguy hiểm tích hợp trong hệ thống.

b) Xác định các tình huống dẫn đến nguy hiểm.

c) Xác định rủi ro liên quan tới nguy hiểm.

d) Xây dựng quy trình quản lý rủi ro hiện có.

6.3.2 Các đầu vào

Đầu vào cho giai đoạn này phải bao gồm các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng các yêu cầu của giai đoạn, đặc biệt là các tài liệu chuyển giao của giai đoạn 2.

6.3.3 Các yêu cầu

6.3.3.1 Yêu cầu 1 của giai đoạn này là phải:

a) Xác định một cách có hệ thống và xếp hạng ưu tiên các nguy hiểm có thể dự đoán được một cách hợp lý liên quan tới hệ thống trong môi trường áp dụng nó, bao gồm các nguy hiểm phát sinh từ:

- Quá trình vận hành bình thường hệ thống;
- Các điều kiện phát sinh sự cố hệ thống;
- Quá trình vận hành khẩn cấp hệ thống;
- Sử dụng sai hệ thống;
- Các tương giao của hệ thống;
- Chức năng của hệ thống;
- Các vấn đề về vận hành, bảo dưỡng và hỗ trợ hệ thống;
- Các xem xét hủy bỏ hệ thống;
- Các yếu tố con người;

- Các vấn đề về sức khỏe nghề nghiệp;
- Môi trường cơ giới;
- Môi trường điện;
- Môi trường tự nhiên, đề cập tới những vấn đề như tuyết, lũ lụt, bão, mưa, lở đất…

b) Xác định chuỗi các tình huống sẽ dẫn tới nguy hiểm.

c) Đánh giá tần suất xuất hiện của từng nguy hiểm (Bảng 2).

d) Đánh giá mức độ nghiêm trọng có khả năng của các hậu quả của từng nguy hiểm (Bảng 3)

e) Đánh giá rủi ro cho hệ thống đối với từng nguy hiểm.

6.3.3.2 Yêu cầu 2 của giai đoạn này là phải xác định và phân loại khả năng chấp nhận rủi ro liên quan tới từng nguy hiểm đã được nhận biết, có xem xét đến rủi ro về mặt xung đột giữa tính sẵn sàng và các yêu cầu về chi phí vòng đời hệ thống.

6.3.3.3 Yêu cầu 3 của giai đoạn này là phải xây dựng Sổ tay nguy hiểm (*Hazard Log*) như là cơ sở để quản lý rủi ro hiện có. Sổ tay nguy hiểm phải được cập nhật, bất kể khi nào xuất hiện thay đổi đối với mọi nguy hiểm đã được nhận biết, hoặc nhận biết được một nguy hiểm mới trong vòng đời hệ thống. Sổ tay nguy hiểm phải có các chi tiết về:

a) Mục tiêu và mục đích của Sổ tay nguy hiểm;

b) Mọi tình huống nguy hiểm và các yếu tố tạo nên;

c) Các hậu quả có khả năng xảy ra và tần suất của các chuỗi tình huống liên quan đến từng nguy hiểm;

d) Rủi ro của từng nguy hiểm;

e) Chỉ tiêu chấp nhận rủi ro cho hệ thống;

f) Các biện pháp được sử dụng để giảm bớt rủi ro về mức chấp nhận được, hoặc loại bỏ rủi ro cho từng tình huống nguy hiểm;

g) Quy trình xem xét khả năng chấp nhận rủi ro;

h) Quy trình xem xét sự hiệu quả của các biện pháp giảm bớt rủi ro;

i) Quy trình báo cáo tai nạn và rủi ro hiện có;

j) Quy trình quản lý Sổ tay nguy hiểm;

k) Các giới hạn của mọi phân tích được tiến hành;

l) Mọi giả thiết được sử dụng trong các phân tích;

m) Mọi giới hạn về độ tin cậy áp dụng cho các dữ liệu được sử dụng trong các phân tích;

n) Các phương pháp, các công cụ và các kĩ thuật được sử dụng;

o) Nhân sự, năng lực liên quan trong quy trình;

6.3.4 Tài liệu chuyển giao

6.3.4.1 Các kết quả của giai đoạn này phải được ghi lại, cùng với mọi giả thiết và các minh chứng được thực hiện trong suốt giai đoạn.

6.3.4.2 Các kết quả của phân tích rủi ro phải được ghi lại trong Sổ tay nguy hiểm.

6.3.4.3 Các tài liệu chuyển giao từ giai đoạn này là đầu vào chính cho các giai đoạn vòng đời hệ thống tiếp theo.

6.3.5 Thẩm tra

6.3.5.1 Các nhiệm vụ thẩm tra dưới đây phải được thực hiện trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi cần là dữ liệu và các thống kê khác, được sử dụng như là đầu vào trong giai đoạn này;

b) Thẩm tra các tài liệu chuyển giao của giai đoạn 3 với các tài liệu chuyển giao của giai đoạn 2;

c) Đánh giá mức độ hoàn thiện của việc đánh giá rủi ro;

d) Đánh giá mức độ phân loại chấp nhận rủi ro;

e) Đánh giá khả năng phù hợp của quá trình ghi lại nguy hiểm đối với hệ thống được xem xét;

f) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn;

g) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.3.5.2 Mọi lỗi hoặc thiếu sót có thể sẽ yêu cầu áp dụng lại một hoặc tất cả các hoạt động của một hoặc nhiều giai đoạn vòng đời hệ thống trước đó.

6.4 Giai đoạn 4: Các yêu cầu hệ thống

6.4.1 Mục tiêu

Mục tiêu của giai đoạn này là để:

a) Quy định các yêu cầu về RAMS tổng thể cho hệ thống.

b) Quy định về việc chứng minh và chỉ tiêu chấp nhận về RAMS cho hệ thống.

c) Xây dựng Chương trình RAM để kiểm soát các nhiệm vụ RAM trong các giai đoạn tiếp theo.

6.4.2 Các đầu vào

Đầu vào cho giai đoạn này phải có tất cả các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng các yêu cầu của giai đoạn, đặc biệt là các tài liệu chuyển giao của giai đoạn 2 và giai đoạn 3.

6.4.3 Các yêu cầu

6.4.3.1 Yêu cầu 1 của giai đoạn này là phải xác định rõ (xem 6.2.3.1) các yêu cầu RAMS tổng thể cho toàn bộ hệ thống. Các yêu cầu về RAMS đối với hệ thống được xem xét phải có:

- Tài liệu xác định hệ thống và các giới hạn;
- Hồ sơ nhiệm vụ;
- Các yêu cầu về chức năng và các yêu cầu về hoạt động hỗ trợ, có cả các yêu cầu về chức năng an toàn và các yêu cầu về tính toàn vẹn an toàn cho từng chức năng an toàn;
- Các yêu cầu nguồn lực cung ứng;
- Các tương giao;
- Môi trường hệ thống;
- Các mức rủi ro chấp nhận được cho các nguy hiểm đã được nhận biết;
- Các biện pháp bên ngoài cần thiết để đạt được các yêu cầu;
- Các yêu cầu hỗ trợ hệ thống;
- Các chi tiết về các giới hạn của phân tích;
- Các chi tiết của mọi giả thiết được đặt ra.

6.4.3.2 Yêu cầu 2 của giai đoạn này là phải quy định (xem 6.2.3.3) các yêu cầu tổng thể để đạt được sự phù hợp với các yêu cầu về RAMS cho hệ thống, bao gồm:

- Chỉ tiêu chấp nhận đối với các yêu cầu tổng thể về RAMS;

- Quy trình chứng minh và chấp nhận đối với các yêu cầu tổng thể về RAMS được hỗ trợ bởi kế hoạch xác nhận RAMS hệ thống, gồm có:

- Mô tả hệ thống;

- Các nguyên tắc xác nhận RAMS được áp dụng cho hệ thống;

- Các thử nghiệm và phân tích RAMS được thực hiện cho việc xác nhận, bao gồm các chi tiết về môi trường, công cụ, thiết bị được yêu cầu…

- Cơ cấu quản lý xác nhận bao gồm các yêu cầu về tính độc lập của các cá nhân;

- Chi tiết về chương trình xác nhận (thứ tự và kế hoạch);

- Các quy trình giải quyết sự không phù hợp.

6.4.3.3 Yêu cầu 3 của giai đoạn này là phải thiết lập Chương trình RAM chi tiết đối với các nhiệm vụ vòng đời hệ thống còn lại (tham khảo 6.2.3.3). Chương trình RAM phải bao gồm các nhiệm vụ được xem là hiệu quả nhất để đạt được các yêu cầu về RAM cho hệ thống xem xét. Chương trình RAM phải được Doanh nghiệp đường sắt và đơn vị công nghiệp phụ trợ đường sắt đồng ý cho hệ thống xem xét và phải được thực hiện trong suốt vòng đời hệ thống. Trong chương trình RAM, nên xem xét đưa ra các nhiệm vụ dưới đây:

a) Sự quản lý, bao gồm các chi tiết về:

- Chính sách và chiến lược để đạt được các yêu cầu về RAM;

- Phạm vi của chương trình;

- Mô tả hệ thống;

- Vòng đời hệ thống và các nhiệm vụ RAM và các quy trình được tiến hành trong vòng đời hệ thống, đặc biệt là thứ tự của các nhiệm vụ RAM để đảm bảo lợi ích tối đa cho thiết kế hệ thống;

- Các vai trò, trách nhiệm và các mối quan hệ của các tổ chức thực hiện các nhiệm vụ trong vòng đời hệ thống;

- Hệ thống phân tích báo cáo hư hỏng và hoạt động sửa chữa (FRACAS) được áp dụng cho hệ thống từ giai đoạn 7 của vòng đời hệ thống (do Doanh nghiệp đường sắt và đơn vị công nghiệp phụ trợ đường sắt phù hợp), có các dữ liệu lưu trữ:
    - Dữ liệu kĩ thuật trên hệ thống;
    - Lý do cho hoạt động bảo dưỡng;
    - Loại hình hoạt động bảo dưỡng;
    - Giờ công và thời gian cho các hoạt động bảo dưỡng;
    - Thời gian nghỉ bảo dưỡng;
    - Số lượng và năng lực của các cá nhân;
    - Các phụ tùng thay thế được sử dụng;
    - Chi phí tiêu dùng;
    - Báo cáo và hoạt động sửa chữa.
- Các sắp xếp để đảm bảo sự phối hợp các yếu tố RAM độc lập;
- Chi tiết của tất cả các tài liệu chuyển giao liên quan tới RAM trong vòng đời hệ thống;
- Chi tiết về các nhiệm vụ chấp nhận RAM;
- Các tương giao với các chương trình và kế hoạch liên quan khác;
- Các liên kết ràng buộc và các giả thiết được đưa ra trong chương trình RAM;
- Bố trí quản lý nhà thầu phụ.

b) Độ tin cậy, gồm:

- Phân tích và dự đoán độ tin cậy, bao gồm:
    - Phân tích chức năng và xác định hư hỏng hệ thống;
    - Phân tích từ trên xuống, ví dụ: phân tích sự cố hình cây và phân tích sơ đồ khối;
    - Phân tích từ dưới lên, ví dụ: Phân tích tác động của các dạng hư hỏng (FMEA);
    - Phân tích hư hỏng hoặc nhiều hư hỏng có nguyên nhân chung;

- Phân tích độ nhạy và các nghiên cứu phi thương mại;
- Phân bổ độ tin cậy;
- Phân tích tương giao giữa máy móc và con người;
- Phân tích áp lực tác động;
- Dự đoán trường hợp xấu nhất và phân tích khả năng chấp nhận.

- Lập kế hoạch cho độ tin cậy, bao gồm:
  - Chương trình xem xét thiết kế độ tin cậy;
  - Chương trình đảm bảo độ tin cậy tổng thành;
  - Chương trình đảm bảo độ tin cậy/chất lượng phần mềm.
- Thử nghiệm độ tin cậy, bao gồm:
  - Thử nghiệm sự gia tăng độ tin cậy, dựa trên sự phát sinh các hư hỏng;
  - Thử nghiệm chứng minh độ tin cậy, dựa trên các dạng hư hỏng đã biết;
  - Phân loại áp lực lên môi trường;
  - Thử nghiệm tuổi thọ của các tổng thành;
  - Thử nghiệm tuổi thọ hệ thống trong suốt quá trình vận hành ban đầu.
- Thu thập dữ liệu về độ tin cậy và đánh giá;
- Phân tích dữ liệu để cải thiện độ tin cậy;

c) Khả năng bảo dưỡng, gồm:

- Phân tích và dự đoán về khả năng bảo dưỡng, bao gồm:
  - Phân tích khả năng bảo dưỡng và thẩm tra;
  - Phân tích nhiệm vụ bảo dưỡng;
  - Các nghiên cứu về khả năng dễ dàng bảo dưỡng và thử nghiệm;
  - Xem xét khả năng duy trì yếu tố con người.

- Lập kế hoạch cho khả năng bảo dưỡng, bao gồm:
    - Chương trình xem xét thiết kế khả năng bảo dưỡng;
    - Thiết lập chiến lược bảo trì, bảo dưỡng;
    - Xem xét các lựa chọn bảo trì, bảo dưỡng tập trung vào độ tin cậy;
    - Chương trình bảo trì phần mềm.
- Đánh giá nguồn lực cung ứng, bao gồm:
    - Xác định các yêu cầu bảo dưỡng;
    - Xác định các chính sách và nguồn lực cung ứng phụ tùng;
    - Nhân lực bảo dưỡng và các phương tiện, thiết bị;
    - Biện pháp phòng ngừa về an toàn cho con người;
    - Các yêu cầu hỗ trợ hệ thống;
    - Các yêu cầu về chương trình đào tạo;
    - Các điều kiện vận chuyển, đóng gói, chuyển giao và lưu trữ hệ thống.
- Thu thập dữ liệu về khả năng bảo dưỡng và đánh giá
- Phân tích dữ liệu để cải thiện khả năng bảo dưỡng.

d) Tính sẵn sàng, bao gồm:

- Phân tích tính sẵn sàng;
- Phân tích độ nhạy và các nghiên cứu phi thương mại;
- Chứng minh tính sẵn sàng trong quá trình vận hành ban đầu;
- Thu thập dữ liệu và đánh giá về tính sẵn sàng;
- Phân tích dữ liệu để cải thiện và dự báo về tính sẵn sàng.

6.4.3.4 Yêu cầu 4 của giai đoạn này phải được bổ sung vào Kế hoạch an toàn để đảm bảo tất cả các nhiệm vụ được lập kế hoạch trong tương lai thống nhất với các yêu cầu RAMS chính của hệ thống.

6.4.4 Tài liệu chuyển giao

6.4.4.1 Các kết quả của giai đoạn này phải được ghi lại, cùng với mọi giả thiết và minh chứng được đưa ra trong suốt giai đoạn.

6.4.4.2 Giai đoạn này phải tạo ra Kế hoạch an toàn và Kế hoạch chấp nhận được cập nhật liên tục.

6.4.4.3 Các tài liệu chuyển giao từ giai đoạn này là đầu vào cho các giai đoạn vòng đời hệ thống tiếp theo.

6.4.5 Thẩm tra

6.4.5.1 Các nhiệm vụ thẩm tra dưới đây phải được thực hiện trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi phù hợp là các dữ liệu và thống kê khác được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này.

b) Thẩm tra các yêu cầu về hệ thống theo các tài liệu chuyển giao có trong giai đoạn 2 và giai đoạn 3, bao gồm các chi phí vòng đời hệ thống.

c) Thẩm tra các yêu cầu về an toàn theo mọi mục tiêu về an toàn và các chính sách an toàn của doanh nghiệp đường sắt.

d) Thẩm tra các yêu cầu về RAM theo mọi mục tiêu về an toàn và các chính sách an toàn của Doanh nghiệp đường sắt.

e) Đánh giá sự phù hợp và sự hoàn chỉnh của Kế hoạch chấp nhận và Kế hoạch xác nhận.

f) Đánh giá sự phù hợp của Chương trình RAM, bao gồm xem xét cả sự phù hợp của mọi nguồn dữ liệu đã được sử dụng.

g) Đánh giá các phương pháp, các công cụ và kĩ thuật được sử dụng trong giai đoạn.

h) Đánh giá năng lực của các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.4.5.2 Mọi lỗi hoặc sự thiếu sót có thể sẽ yêu cầu áp dụng lại một số hoặc tất cả các hoạt động của một hoặc nhiều giai đoạn vòng đời hệ thống trước đó.

6.5 Giai đoạn 5: Phân bổ các yêu cầu hệ thống

6.5.1 Mục tiêu

Mục đích của giai đoạn này là để:

a) Phân bổ các yêu cầu tổng hợp về RAMS cho hệ thống đến các hệ thống con được chỉ định, các tổng thành và các yếu tố bên ngoài.

b) Xác định chỉ tiêu chấp nhận RAMS cho các hệ thống con được chỉ định, các tổng thành và các yếu tố bên ngoài.

6.5.2 Các đầu vào

Đầu vào cho giai đoạn này bao gồm tất cả các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng các yêu cầu của giai đoạn, đặc biệt là các tài liệu chuyển giao được tạo ra trong giai đoạn 4.

6.5.3 Các yêu cầu

6.5.3.1 Yêu cầu 1 của giai đoạn này là phải:

a) Phân bổ các yêu cầu về chức năng cho các hệ thống con được chỉ định, các tổng thành và các yếu tố bên ngoài.

b) Phân bổ các yêu cầu về an toàn đến các hệ thống con được chỉ định, các tổng thành và các yếu tố giảm bớt rủi ro bên ngoài.

c) Quy định các hệ thống con, các tổng thành và các yếu tố bên ngoài được chỉ định để đạt được các yêu cầu RAM hệ thống một cách hoàn chỉnh, bao gồm tác động của hư hỏng có chung nguyên nhân và của nhiều hư hỏng.

d) Xem xét chương trình RAM.

6.5.3.2 Yêu cầu 2 của giai đoạn này là phải chỉ rõ các yêu cầu phù hợp với các yêu cầu của hệ thống con, tổng thành và các yếu tố bên ngoài, bao gồm:

- Chỉ tiêu chấp nhận đối với các yêu cầu của hệ thống con, tổng thành và các yếu tố bên ngoài;

- Quy trình chứng minh và chấp nhận và các quy trình cho các yêu cầu đối với hệ thống con, tổng thành và các yếu tố bên ngoài.

6.5.3.3 Yêu cầu 3 của giai đoạn này là phải xem xét và cập nhật Kế hoạch an toàn và Kế hoạch xác nhận để đảm bảo rằng các nhiệm vụ được lập kế hoạch là thống nhất với các yêu cầu của việc phân bổ hệ thống dưới đây. Vấn đề chính cần quan tâm bao gồm các yêu cầu về sự độc lập của các cá nhân và kiểm soát các tương giao hệ thống tại những vị trí chức năng an toàn có thể bị giảm giá trị.

6.5.4 Tài liệu chuyển giao

6.5.4.1 Các kết quả của giai đoạn này phải được ghi lại, cùng với mọi giả thiết và minh chứng được đưa ra trong suốt giai đoạn.

6.5.4.2 Giai đoạn này phải tạo ra một Kế hoạch an toàn được cập nhật.

6.5.4.3 Các tài liệu tạo ra trong giai đoạn này phải có các yêu cầu hệ thống đã được phân bổ cho các hệ thống con được chỉ định, các tổng thành và các yếu tố bên ngoài.

6.5.4.4 Tài liệu chuyển giao từ giai đoạn này là đầu vào chính đối với các giai đoạn vòng đời hệ thống tiếp theo.

6.5.5 Thẩm tra

6.5.5.1 Các nhiệm vụ thẩm tra dưới đây phải được thực hiện trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi phù hợp là các dữ liệu và thống kê khác được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này;

b) Thẩm tra các yêu cầu của hệ thống, hệ thống con, tổng thành và các yếu tố bên ngoài theo các tài liệu chuyển giao tạo ra trong giai đoạn 4, bao gồm việc xem xét các yêu cầu dựa trên chi phí vòng đời hệ thống của hệ thống;

c) Thẩm tra cấu trúc kết hợp tổng thể các hệ thống con được chỉ định, các tổng thành và các yếu tố bên ngoài để đảm bảo nó thỏa mãn các yêu cầu về RAMS cho toàn bộ hệ thống;

d) Thẩm tra các yêu cầu về RAMS cho các hệ thống con, các tổng thành và các yếu tố bên ngoài để đảm bảo có khả năng theo dõi theo vết theo các yêu cầu RAMS cho hệ thống;

e) Thẩm tra các yêu cầu về RAMS cho các hệ thống con, các tổng thành và các yếu tố bên ngoài để đảm bảo sự hoàn chỉnh và tính thống nhất giữa các chức năng;

f) Thẩm tra Kế hoạch an toàn và Kế hoạch xác nhận được cải tiến để đảm bảo khả năng áp dụng liên tục của nó;

g) Đánh giá sự phù hợp của các phương pháp, các công cụ và kĩ thuật được sử dụng trong giai đoạn này;

h) Đánh giá về năng lực của các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.5.5.2 Mọi lỗi hoặc sự thiếu sót có thể sẽ yêu cầu áp dụng lại một số hoặc tất cả các hoạt động của một hoặc nhiều giai đoạn vòng đời hệ thống trước đó.

6.6 Giai đoạn 6: Thiết kế và thực hiện

6.6.1 Mục tiêu

Mục tiêu của giai đoạn này là để:

a) Tạo ra các hệ thống con và các tổng thành thỏa mãn các yêu cầu về RAMS.

b) Chứng minh các hệ thống con và các tổng thành thỏa mãn các yêu cầu về RAMS.

c) Thiết lập các kế hoạch cho các nhiệm vụ vòng đời hệ thống trong tương lai có liên quan tới RAMS.

6.6.2 Các đầu vào

Đầu vào cho giai đoạn này phải có tất cả các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng các yêu cầu, đặc biệt là các tài liệu chuyển giao tạo ra trong giai đoạn 4 và giai đoạn 5.

6.6.3 Các yêu cầu

6.6.3.1 Yêu cầu 1 của giai đoạn này là phải thiết kế các hệ thống con và các tổng thành để đáp ứng các yêu cầu về RAMS.

6.6.3.2 Yêu cầu 2 của giai đoạn này là phải xác định thiết kế các hệ thống con và các tổng thành để đáp ứng các yêu cầu của RAMS.

6.6.3.3 Yêu cầu 3 của giai đoạn này là phải thiết lập ra các kế hoạch, theo nội dung về RAMS, đối với các nhiệm vụ vòng đời hệ thống tương lai, bao gồm:

- Lắp đặt;
- Thử hoạt động;
- Vận hành và bảo dưỡng, bao gồm xác định các quy trình vận hành và bảo dưỡng;
- Thu thập dữ liệu và đánh giá trong quá trình vận hành.

6.6.3.4 Yêu cầu 4 của giai đoạn này là phải xác định, thẩm tra và thiết lập quy trình sản xuất có khả năng tạo ra các hệ thống con và các tổng thành đã được xác nhận về RAMS, xem xét việc sử dụng:

- Đánh giá sơ bộ ứng suất môi trường;
- Thử nghiệm việc cải tiến RAM;
- Kiểm tra và thử nghiệm các dạng hư hỏng có liên quan tới RAMS;
- Thực hiện yêu cầu 4 của Kế hoạch an toàn (mục d của 6.2.3.4).

6.6.3.5 Yêu cầu 5 của giai đoạn này là phải:

a) Chuẩn bị Hồ sơ an toàn chung cho hệ thống để đưa ra kết luận rằng hệ thống được thiết kế và không phụ thuộc vào khai thác áp dụng, thỏa mãn các yêu cầu về an toàn. Hồ sơ an toàn phải được chấp thuận bởi Doanh nghiệp đường sắt và nên bao gồm:

- Giới thiệu tổng quan về hệ thống;

- Tài liệu tóm tắt hoặc tham chiếu về các yêu cầu về an toàn, bao gồm việc xem xét về chứng minh SIL đối với các chức năng an toàn;

- Tài liệu tóm tắt các biện pháp kiểm soát quản lý về chất lượng và an toàn được chấp nhận trong vòng đời hệ thống;

- Tài liệu tóm tắt các nhiệm vụ đánh giá và kiểm toán an toàn;

- Tài liệu tóm tắt các nhiệm vụ phân tích an toàn;

- Tài liệu tổng quát về các biện pháp kĩ thuật an toàn được sử dụng trong hệ thống;

- Báo cáo thẩm tra quy trình sản xuất;

- Tài liệu về sự phù hợp với các yêu cầu về an toàn, bao gồm tất cả các yêu cầu về SIL của hệ thống.

- Tài liệu tóm tắt tất cả các giới hạn và các ràng buộc áp dụng cho hệ thống;

- Mọi trường hợp ngoại lệ đặc biệt (hoặc cụ thể) khác với các yêu cầu thông thường của tiêu chuẩn này và được bảo đảm bằng hợp đồng.

b) Chuẩn bị Hồ sơ an toàn ứng dụng cho hệ thống, nếu phù hợp tại giai đoạn này. Hồ sơ an toàn ứng dụng xây dựng trên cơ sở của Hồ sơ an toàn chung, chứng minh thiết kế của hệ thống và quá trình thực hiện thỏa mãn các yêu cầu về an toàn ở một mức độ ứng dụng cụ thể, bao gồm các giai đoạn lắp đặt và thử nghiệm. Yêu cầu Hồ sơ an toàn ứng dụng có sự chứng nhận của Doanh nghiệp đường sắt và nên bao gồm:

- Tất cả các thông tin bổ sung cần thiết cho việc thuyết minh hệ thống an toàn đối với loại hình ứng dụng được xem xét;

- Mọi giới hạn và ràng buộc liên quan tới việc ứng dụng hệ thống.

6.6.4 Tài liệu chuyển giao

6.6.4.1 Các kết quả của giai đoạn này phải được lưu lại, cùng với mọi giải thiết và các minh chứng được đưa ra trong suốt giai đoạn.

6.6.4.2 Duy trì việc ghi lại mọi nhiệm vụ xác nhận RAMS được tiến hành trong giai đoạn.

6.6.4.3 Phải tạo ra các kế hoạch chi tiết đối với các nhiệm vụ vòng đời hệ thống tương lai, theo nội dung về RAMS.

6.6.4.4 Phải tạo ra trong giai đoạn này các quy trình vận hành và bảo dưỡng, bao gồm tất cả các thông tin liên quan cho việc cung ứng các phụ tùng thay thế, đặc biệt là các hạng mục liên quan tới an toàn.

6.6.4.5 Hồ sơ an toàn chung phải được tạo ra trong giai đoạn này.

6.6.4.6 Hồ sơ an toàn ứng dụng có thể được tạo ra trong giai đoạn này.

6.6.4.7 Các tài liệu chuyển giao trong giai đoạn này là đầu vào chủ yếu cho các giai đoạn vòng đời hệ thống sau này.

6.6.5 Thẩm tra

6.6.5.1 Các nhiệm vụ thẩm tra dưới đây phải được tiến hành trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi phù hợp là dữ liệu và các thống kê khác, được sử dụng là đầu vào của các nhiệm vụ trong giai đoạn này.

b) Thẩm tra, bằng phân tích và thử nghiệm xem thiết kế hệ thống con và tổng thành thỏa mãn các yêu cầu về RAMS.

c) Thẩm tra, bằng phân tích và thử nghiệm xem xét việc nhận biết các hệ thống con và các tổng thành có thỏa mãn các thiết kế.

d) Xác nhận quá trình nhận biết các hệ thống con và tổng thành để đảm bảo quá trình nhận biết thỏa mãn các chỉ tiêu chấp nhận về RAMS cho hệ thống con và các tổng thành, bao gồm các yêu cầu về vòng đời hệ thống.

e) Thẩm tra, bằng phân tích và kiểm tra xem các sắp xếp bố trí sản xuất có tạo ra được các hệ thống con và các tổng thành đã được xác nhận RAMS.

f) Thẩm tra tất cả các kế hoạch hoạt động vòng đời hệ thống tương lai có thống nhất với các yêu cầu về RAMS cho hệ thống, bao gồm các yêu cầu về chi phí vòng đời hệ thống.

g) Đánh giá sự phù hợp và sự hoàn chỉnh của Hồ sơ an toàn chung và khi cần là Hồ sơ an toàn ứng dụng.

h) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn này.

i) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

j) Đảm bảo khả năng áp dụng liên tục của kế hoạch xác nhận RAMS.

6.6.5.2 Mọi lỗi hoặc thiếu sót có thể sẽ yêu cầu áp dụng lại của một số hoặc tất cả các hoạt động của một hoặc nhiều giai đoạn vòng đời hệ thống trước đó.

6.7 Giai đoạn 7: Sản xuất

6.7.1 Mục tiêu

Mục tiêu của giai đoạn này là để:

a) Thực hiện quy trình sản xuất tạo ra các hệ thống con và các tổng thành được xác nhận RAMS;

b) Thiết lập các sắp xếp đảm bảo quá trình lấy RAMS làm trung tâm;

c) Thiết lập các sắp xếp hỗ trợ về RAMS của hệ thống con và tổng thành.

6.7.2 Các đầu vào

Đầu vào của giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng yêu cầu, đặc biệt là các tài liệu chuyển giao về thiết kế được tạo ra trong giai đoạn 6.

6.7.3 Các yêu cầu

6.7.3.1 Yêu cầu 1 của giai đoạn này là phải thẩm tra và thực hiện quy trình sản xuất.

6.7.3.2 Yêu cầu 2 của giai đoạn này là phải thiết lập các bố trí sắp xếp hỗ trợ hệ thống con và tổng thành, bao gồm:

- Chuẩn bị, thẩm tra và xác nhận tài liệu hỗ trợ về RAMS của hệ thống con và tổng thành;
- Chuẩn bị, thẩm tra và xác nhận các quy trình vận hành và bảo dưỡng theo nội dung về RAMS;
- Chuẩn bị, thẩm tra và xác nhận tài liệu đào tạo về hệ thống con và tổng thành theo nội dung về RAMS.
- Hồ sơ, các quy trình và tài liệu đào tạo trên phải được xem xét lại ở tất cả các giai đoạn sau này.

6.7.3.3 Yêu cầu 3 của giai đoạn này nếu có thể phù hợp là:

a) Lập kế hoạch sản xuất để đáp ứng các yêu cầu.

b) Thực hiện việc sản xuất để đáp ứng các yêu cầu.

c) Thực hiện các đảm bảo quy trình RAMS để tránh được các dạng hư hỏng tiềm ẩn liên quan tới RAMS.

6.7.4 Tài liệu chuyển giao

6.7.4.1 Các kết quả của giai đoạn này phải được lưu lại, cùng với mọi giả thiết và minh chứng được thực hiện trong suốt giai đoạn.

6.7.4.2 Phải duy trì biên bản ghi lại tất cả các nhiệm vụ xác nhận RAMS được tiến hành trong giai đoạn.

6.7.4.3 Các tài liệu chuyển giao từ giai đoạn này là đầu vào chính cho các giai đoạn vòng đời hệ thống sau.

6.7.5 Thẩm tra

6.7.5.1 Các nhiệm vụ thẩm tra dưới đây phải được thực hiện trong giai đoạn này:

a) Đánh giá về sự phù hợp của thông tin và khi phù hợp là dữ liệu và các thống kê khác, được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này.

b) Thẩm tra xem các tài liệu hỗ trợ RAMS có chính xác, đầy đủ và thống nhất với các yêu cầu về chi phí vòng đời hệ thống và các yêu cầu về chỉ tiêu RAMS được xác định cho hệ thống.

c) Đánh giá để đảm bảo tạo ra các sản phẩm thỏa mãn các yêu cầu của hệ thống.

d) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn.

e) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.7.5.2 Mọi lỗi hoặc sự thiếu sót có thể sẽ yêu cầu áp dụng lại một số hoặc tất cả các hoạt động của một hoặc nhiều giai đoạn vòng đời hệ thống trước đây.

6.8 Giai đoạn 8: Lắp đặt

6.8.1 Mục tiêu

Mục tiêu của giai đoạn này là phải:

a) Lắp ráp và lắp đặt kết hợp tất cả các hệ thống con và các tổng thành được yêu cầu để tạo nên hệ thống hoàn chỉnh.

b) Triển khai các bố trí sắp xếp hỗ trợ hệ thống.

6.8.2 Các đầu vào

Đầu vào của giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng các yêu cầu, đặc biệt là Kế hoạch lắp đặt được chuẩn bị trong giai đoạn 6, các hệ thống con và các tổng thành được sản xuất trong giai đoạn 7 và tài liệu hỗ trợ RAMS được chuẩn bị trong giai đoạn 7.

6.8.3 Các yêu cầu

6.8.3.1 Yêu cầu 1 của giai đoạn này là phải lắp ráp và lắp đặt kết hợp tất cả các hệ thống con, các tổng thành và các yếu tố bên ngoài được yêu cầu để tạo nên hệ thống hoàn chỉnh theo như Kế hoạch lắp đặt.

6.8.3.2 Yêu cầu 2 của giai đoạn này là phải ghi chép lại quy trình lắp đặt, bao gồm:

- Xem xét các kế hoạch theo nội dung yêu cầu 3 của giai đoạn Thiết kế và thực hiện (6.6.3.3);
- Các nhiệm vụ lắp đặt;
- Hoạt động được thực hiện để giải quyết các hư hỏng và các vấn đề không tương thích.

6.8.3.3 Yêu cầu 3 của giai đoạn này là phải xem xét và cập nhật Kế hoạch an toàn sau khi hoàn thiện lắp đặp để đảm bảo mọi thay đổi đối với hệ thống hoặc các quy trình được ghi chép lại và được quản lý hiệu quả trong các nhiệm vụ vòng đời hệ thống tương lai.

6.8.3.4 Yêu cầu 4 của giai đoạn này là phải:

a) Triển khai đào tạo nhân viên;

b) Tạo ra các quy trình hỗ trợ;

c) Dự phòng phụ tùng thay thế;

d) Dự phòng các dụng cụ.

6.8.4 Tài liệu chuyển giao

6.8.4.1 Các kết quả của giai đoạn này phải được ghi lại, cùng với mọi giả thiết và minh chứng được thực hiện trong giai đoạn.

6.8.4.2 Phải duy trì biên bản ghi lại mọi nhiệm vụ xác nhận RAMS được tiến hành trong giai đoạn, bao gồm cả hoạt động lắp đặt.

6.8.4.3 Phải tạo ra một kế hoạch an toàn được cập nhật trong giai đoạn này.

6.8.4.4 Các tài liệu chuyển giao từ giai đoạn này là đầu vào chính cho các giai đoạn vòng đời hệ thống sau.

6.8.5 Thẩm tra

6.8.5.1 Các nhiệm vụ thẩm tra dưới đây phải được thực hiện trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi phù hợp là dữ liệu và các thống kê khác được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này;

b) Thẩm tra xem hoạt động lắp đặt được thực hiện có phù hợp với Kế hoạch lắp đặt;

c) Thẩm tra, bằng phân tích và thử nghiệm xem hệ thống được lắp đặt có đáp ứng các yêu cầu về RAMS;

d) Đánh giá Kế hoạch an toàn để đảm bảo khả năng áp dụng liên tục của nó;

e) Đánh giá sự phù hợp và tính hiệu quả của các bố trí sắp xếp hỗ trợ hệ thống;

f) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn;

g) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.8.5.2 Mọi lỗi hoặc sự thiếu sót có thể sẽ yêu cầu áp dụng lại một số hoặc tất cả các hoạt động của một hoặc nhiều giai đoạn vòng đời hệ thống trước đây.

6.9 Giai đoạn 9: Xác nhận hệ thống (bao gồm chấp nhận an toàn và thử hoạt động)

6.9.1 Mục tiêu

6.9.1.1 Mục tiêu của giai đoạn này là để:

a) Xác nhận việc kết hợp toàn bộ các hệ thống con, các tổng thành và các biện pháp giảm bớt rủi ro bên ngoài thỏa mãn các yêu cầu về RAMS cho hệ thống.

b) Thử hoạt động kết hợp toàn bộ các hệ thống con, các tổng thành và các biện pháp giảm bớt rủi ro bên ngoài.

c) Chuẩn bị Hồ sơ an toàn ứng dụng cụ thể đối với hệ thống, nếu được chấp nhận phù hợp.

d) Chuẩn bị việc thu thập và đánh giá dữ liệu.

6.9.1.2 Chú ý quan trọng rằng các yêu cầu của giai đoạn 10 - Chấp nhận hệ thống, có thể được tích hợp trong các yêu cầu của giai đoạn 9 này, nếu phù hợp với hệ thống được xem xét. Nếu xảy ra trường

hợp này, các tài liệu chuyển giao từ giai đoạn 9 này phải chứng minh các yêu cầu của giai đoạn 10 đã được đáp ứng đầy đủ tương ứng trong quá trình xác định của giai đoạn 9.

6.9.2 Các đầu vào

Đầu vào cho giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là các dữ liệu cần thiết để đáp ứng yêu cầu, đặc biệt là các yêu cầu hệ thống được tạo ra trong giai đoạn 4, Kế hoạch thẩm tra và xác nhận được tạo ra trong giai đoạn 4, Kế hoạch thử hoạt động được tạo ra trong giai đoạn 6 và tài liệu đào tạo được chuẩn bị trong giai đoạn 7.

6.9.3 Các yêu cầu

6.9.3.1 Yêu cầu 1 của giai đoạn này là phải xác nhận sự kết hợp toàn bộ các hệ thống con, các tổng thành và các biện pháp giảm bớt rủi ro bên ngoài theo như Kế hoạch xác nhận và ghi lại quá trình xác nhận, bao gồm:

- Chi tiết về các nhiệm vụ xác nhận RAMS theo các tiêu chí chấp nhận, bao gồm các chứng minh RAM và phân tích về an toàn;

- Chi tiết về các quá trình, công cụ, thiết bị được sử dụng trong các nhiệm vụ xác nhận theo các tiêu chí chấp nhận;

- Kết quả của các nhiệm vụ xác nhận đối với tất cả các tiêu chí chấp nhận;

- Mọi giới hạn và ràng buộc áp dụng đối với hệ thống;

- Các hoạt động được tiến hành để xử lý các hư hỏng và sự không tương thích.

6.9.3.2 Yêu cầu 2 của giai đoạn này là phải:

a) Thử hoạt động sự kết hợp các hệ thống con, các tổng thành và các biện pháp giảm bớt rủi ro bên ngoài theo như Kế hoạch thử hoạt động và ghi lại quá trình thử hoạt động, bao gồm:

- Các nhiệm vụ thử hoạt động;

- Các nhiệm vụ đánh giá và báo cáo hư hỏng;

- Hoạt động được thực hiện để giải quyết các hư hỏng và sự không phù hợp;

- Chi tiết về các giới hạn hoặc ràng buộc khi sử dụng hệ thống.

b) Nếu được yêu cầu, tiến hành thời gian vận hành thử thách để đảm bảo giải quyết các vấn đề hệ thống trong khai thác. Nếu quá trình sử dụng trong thời gian vận hành thử thách là một phần cho việc

chấp nhận hệ thống, thì phải đưa ra các xem xét cần thiết cho việc chứng minh an toàn hệ thống trước khi vận hành hệ thống trong thời kì khai thác chính thức.

6.9.3.3 Yêu cầu 3 của giai đoạn này là phải chuẩn bị Hồ sơ an toàn ứng dụng cho hệ thống để thuyết minh hệ thống thỏa mãn các yêu cầu về an toàn, như được áp dụng cụ thể trong hệ thống đường sắt này, nếu chưa được chuẩn bị trong giai đoạn 6 (mục 2 của 6.6.3.5). Hồ sơ an toàn ứng dụng sẽ yêu cầu sự chứng nhận của doanh nghiệp đường sắt và bao gồm:

- Tài liệu mô tả tổng quan hệ thống;

- Tài liệu tổng hợp hoặc tham chiếu đến các yêu cầu về an toàn, bao gồm việc xem xét các chứng minh SIL hoặc các chức năng an toàn trong khi khai thác;

- Tài liệu tổng hợp về các kiểm soát quản lý chất lượng và an toàn được chấp nhận trong vòng đời hệ thống;

- Tài liệu tổng hợp về các nhiệm vụ đánh giá an toàn và kiểm toán an toàn;

- Tài liệu tổng hợp về các nhiệm vụ phân tích an toàn;

- Tài liệu tổng quan về các biện pháp kĩ thuật an toàn được sử dụng trong hệ thống;

- Tài liệu về sự phù hợp đầy đủ các yêu cầu an toàn cho hệ thống, có cả sự phù hợp đầy đủ với các yêu cầu SIL của việc hệ thống đường sắt, bao gồm cả việc thực hiện trong quá trình hệ thống đường sắt cụ thể;

- Tài liệu tổng hợp mọi giới hạn và ràng buộc áp dụng cho việc khai thác.

6.9.3.4 Yêu cầu 4 của giai đoạn này là phải thiết lập và thực hiện quá trình thu thập và đánh giá dữ liệu vận hành làm đầu vào cho quy trình cải tiến nâng cấp hệ thống.

6.9.4 Tài liệu chuyển giao

6.9.4.1 Các kết quả của giai đoạn này phải được ghi chép lại, cùng với mọi giả thiết và chứng minh được thực hiện trong suốt giai đoạn.

6.9.4.2 Phải duy trì việc ghi lại tất cả các nhiệm vụ xác nhận RAMS được tiến hành trong giai đoạn, bao gồm hoạt động đưa vào khai thác.

6.9.4.3 Phải tạo ra một Hồ sơ an toàn ứng dụng cụ thể cho hệ thống trong giai đoạn này.

6.9.4.4 Phải duy trì việc ghi lại tất cả các Nhiệm vụ chấp nhận được tiến hành trong giai đoạn này.

6.9.4.5 Các tài liệu chuyển giao từ giai đoạn này là đầu vào chính cho các giai đoạn vòng đời hệ thống sau này.

6.9.5 Thẩm tra

6.9.5.1 Các nhiệm vụ thẩm tra quy trình dưới đây phải được thực hiện trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi cần là dữ liệu và các thống kê khác, được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này.

b) Thẩm tra và xác nhận, bằng phân tích và thử nghiệm xem hệ thống được lắp đặt có đáp ứng các yêu cầu về RAMS. Cần chú ý đối với một số hệ thống đường sắt, việc chấp nhận Hồ sơ an toàn ứng dụng cụ thể sẽ được yêu cầu trước các hoạt động lắp đặp và thử hoạt động.

c) Thẩm tra việc thử hoạt động có được thực hiện phù hợp với Kế hoạch thử hoạt động.

d) Đánh giá sự phù hợp và hiệu quả của hệ thống thu thập dữ liệu vận hành.

e) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn.

f) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn này

6.9.5.2 Mọi lỗi hoặc thiếu sót có thể sẽ yêu cầu áp dụng lại một số hoặc tất cả các hoạt động của một hoặc nhiều giai đoạn vòng đời hệ thống trước đây.

6.10 Giai đoạn 10: Chấp nhận hệ thống

6.10.1 Mục tiêu

Mục tiêu của giai đoạn này là để:

a) Đánh giá sự phù hợp của việc kết hợp các hệ thống con, các tổng thành và các biện pháp giảm bớt rủi ro bên ngoài với các yêu cầu tổng hợp về RAMS của hệ thống hoàn chỉnh.

b) Chấp nhận hệ thống để đưa vào khai thác.

6.10.2 Các đầu vào

Đầu vào của giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là dữ liệu cần thiết để đáp ứng yêu cầu, đặc biệt là các yêu cầu hệ thống được chuẩn bị trong giai đoạn 4, Kế hoạch thẩm tra và xác nhận và Kế hoạch chấp nhận được chuẩn bị trong giai đoạn 4 và biên bản ghi lại các nhiệm vụ thẩm tra và xác nhận được chuẩn bị trong giai đoạn 9.

6.10.3 Các yêu cầu

6.10.3.1 Yêu cầu 1 của giai đoạn này là phải đánh giá tất cả các nhiệm vụ thẩm tra và xác nhận, cụ thể là việc thẩm tra và xác nhận RAM và Hồ sơ an toàn ứng dụng cụ thể phù hợp với Kế hoạch chấp nhận hệ thống.

6.10.3.2 Nếu phù hợp, yêu cầu 2 của giai đoạn này là phải chấp nhận chính thức hệ thống được đưa vào khai thác.

6.10.3.3 Yêu cầu 3 của giai đoạn này là phải xem xét và cập nhật Sổ tay nguy hiểm, để ghi lại mọi nguy hiểm còn lại được xác định trong quá trình xác nhận hoặc nhấp nhận hệ thống và để đảm bảo các rủi ro từ những nguy hiểm này được quản lý hiệu quả.

6.10.4 Tài liệu chuyển giao

6.10.4.1 Các kết quả của giai đoạn này phải được ghi lại, cùng với mọi giả thiết và chứng minh được thực hiện trong suốt giai đoạn.

6.10.4.2 Phải duy trì việc ghi lại tất cả các nhiệm vụ chấp nhận được tiến hành trong giai đoạn.

6.10.4.3 Phải tạo ra một Sổ tay nguy hiểm được cập nhật trong giai đoạn này.

6.10.4.4 Các tài liệu chuyển giao từ giai đoạn này là đầu vào chính cho các giai đoạn vòng đời hệ thống sau.

6.10.5 Thẩm tra

6.10.5.1 Các nhiệm vụ thẩm tra dưới đây phải được tiến hành trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi cần là dữ liệu và các thống kê khác, được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này;

b) Chấp nhận bằng phân tích và thử nghiệm việc hệ thống đáp ứng các yêu cầu về RAMS, bao gồm các yêu cầu về chi phí vòng đời hệ thống;

c) Thẩm tra hoạt động chấp nhận có được tiến hành phù hợp với Kế hoạch chấp nhận;

d) Đánh giá khả năng áp dụng liên tục của kế hoạch an toàn được sửa đổi;

e) Đánh giá để đảm bảo mọi nguy hiểm còn lại được quản lý hiệu quả;

f) Đánh giá sự phù hợp và sự hoàn chỉnh của Hồ sơ an toàn ứng dụng cụ thể;

g) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn;

h) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.10.5.2 Mọi lỗi hoặc thiếu sót có thể sẽ yêu cầu áp dụng lại một số hoặc tất cả các hoạt động của một hoặc nhiều giai đoạn vòng đời hệ thống trước đây.

6.11 Giai đoạn 11: Vận hành và bảo dưỡng

6.11.1 Mục tiêu

Mục tiêu của giai đoạn này là phải vận hành (trong các giới hạn cụ thể), duy trì và hỗ trợ quá trình kết hợp các hệ thống con, các tổng thành và các biện pháp giảm bớt rủi ro bên ngoài sao cho đảm bảo sự phù hợp với các yêu cầu RAMS hệ thống.

6.11.2 Các đầu vào

Đầu vào cho giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là dữ liệu cần thiết để đáp ứng yêu cầu, đặc biệt là các quy trình vận hành và bảo dưỡng được chuẩn bị trong gian đoạn 6.

6.11.3 Các yêu cầu

6.11.3.1 Yêu cầu 1 của giai đoạn này là phải giám sát sự hoạt động hệ thống và thực hiện các quy trình vận hành và bảo dưỡng, đặc biệt quan tâm tới các vấn đề về chi phí vòng đời hệ thống và tính năng hoạt động của hệ thống.

6.11.3.2 Yêu cầu 2 của giai đoạn này là phải đảm bảo sự phù hợp với các yêu cầu về RAMS hệ thống trong suốt giai đoạn, bằng cách:

a) Xem xét và cập nhật thường xuyên các quy trình vận hành và bảo dưỡng;

b) Xem xét thường xuyên các tài liệu hướng dẫn huấn luyện hệ thống;

c) Xem xét và cập nhật thường xuyên Sổ tay nguy hiểm và Hồ sơ an toàn;

d) Cung ứng nguồn lực hiệu quả, bao gồm các phụ tùng thay thế, các công cụ, hiệu chuẩn, các quá trình bảo dưỡng tập trung vào RAMS.

e) Duy trì việc báo cáo hư hỏng và hệ thống hoạt động khắc phục (FRACAS).

6.11.4 Tài liệu chuyển giao

6.11.4.1 Duy trì việc ghi lại tất cả các nhiệm vụ RAMS được thực hiện trong giai đoạn, cùng với mọi giả thiết và các chứng minh được tiến hành trong suốt giai đoạn.

6.11.4.2 Tài liệu hệ thống phải được cập nhật trong giai đoạn này cho phù hợp.

6.11.4.3 Các tài liệu chuyển giao của giai đoạn này là đầu vào chính cho các giai đoạn vòng đời hệ thống sau.

6.11.5 Thẩm tra

Các nhiệm vụ thẩm tra dưới đây phải được tiến hành trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi phù hợp là dữ liệu và các thống kê khác được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này.

b) Thẩm tra xem các thay đổi trong bố trí sắp xếp hỗ trợ có thống nhất với các yêu cầu về RAMS hệ thống và các yêu cầu về chi phí vòng đời hệ thống.

c) Đánh giá sự phù hợp của các phương pháp, các công cụ và kĩ thuật được sử dụng trong giai đoạn.

d) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.12 Giai đoạn 12: Giám sát hoạt động

6.12.1 Mục tiêu

Mục tiêu của giai đoạn này là phải duy trì độ tin cậy trong đặc tính RAMS của hệ thống.

6.12.2 Các đầu vào

Đầu vào cho giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là dữ liệu cần thiết để đáp ứng yêu cầu, đặc biệt là các yêu cầu RAMS hệ thống và dữ liệu hỗ trợ hệ thống.

6.12.3 Các yêu cầu

6.12.3.1 Yêu cầu 1 của giai đoạn này là phải thiết lập, thực hiện và xem xét thường xuyên quy trình về:

- Thu thập các thống kê về RAMS và hoạt động vận hành;
- Thu thập, phân tích và đánh giá sự hoạt động và các dữ liệu về RAMS;
- Kiểm tra xem các giả thiết được đưa ra trong Hồ sơ an toàn vẫn còn đúng và chính xác.

6.12.3.2 Yêu cầu 2 của giai đoạn này là phải phân tích dữ liệu và các thống kê về sự hoạt động và RAMS đối với các tác động của:

- Các quy trình vận hành và bảo dưỡng mới;
- Các thay đổi trong nguồn lực cung ứng cho hệ thống.

6.12.4 Tài liệu chuyển giao

6.12.4.1 Duy trì việc ghi lại các nhiệm vụ giám sát hoạt động được thực hiện trong giai đoạn, cùng với mọi giả thiết và chứng minh được tiến hành trong suốt giai đoạn.

6.12.4.2 Tài liệu hỗ trợ hệ thống có thể được cập nhật trong giai đoạn này.

6.12.4.3 Các tài liệu chuyển giao từ giai đoạn này là đầu vào chính cho các giai đoạn vòng đời hệ thống sau này.

6.12.5 Thẩm tra

Các nhiệm vụ thẩm tra quy trình dưới đây phải được tiến hành trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi phù hợp là các dữ liệu và các thống kê khác, được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này.

b) Thẩm tra xem các thay đổi trong bố trí sắp xếp hỗ trợ có thống nhất với các yêu cầu RAMS hệ thống và các yêu cầu về chi phí vòng đời hệ thống.

c) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn.

d) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

6.13 Giai đoạn 13: Thay đổi và cải tiến

6.13.1 Mục tiêu

Mục tiêu của giai đoạn này là phải kiểm soát các nhiệm vụ thay đổi và cải tiến hệ thống để duy trì các yêu cầu về RAMS hệ thống.

6.13.2 Các đầu vào

Đầu vào cho giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là dữ liệu cần thiết để đáp ứng các yêu cầu.

6.13.3 Các yêu cầu

6.13.3.1 Yêu cầu 1 của giai đoạn này là phải thiết lập ra một kế hoạch an toàn.

6.13.3.2 Yêu cầu 2 của giai đoạn này là phải thiết lập, thực hiện và xem xét thường xuyên quy trình kiểm soát các thay đổi và cải tiến hệ thống, theo nội dung về RAMS, bao gồm:

- Kiểm soát qua việc sử dụng bắt buộc mô hình vòng đời hệ thống phù hợp đối với tất cả các nhiệm vụ thay đổi và cải tiến;

- Yêu cầu thiết lập quy trình để thẩm tra, xác nhận và chấp nhận đặc tính RAMS của việc thay đổi và cải tiến hệ thống sau đó;

- Yêu cầu phân tích các lý do cho sự thay đổi;

- Yêu cầu thực hiện phân tích ảnh hưởng đến RAMS của thay đổi, bao gồm tác động lên các yêu cầu về chi phí vòng đời hệ thống;

- Yêu cầu lập kế hoạch thực hiện thay đổi và chấp nhận sau đó;

- Yêu cầu ghi lại các nhiệm vụ thay đổi và cải tiến;

- Yêu cầu cập nhật tất cả các tài liệu hệ thống bị ảnh hưởng.

6.13.4 Tài liệu chuyển giao

6.13.4.1 Tài liệu chuyển giao chính từ giai đoạn này là một hệ thống đã được xác nhận, thay đổi.

6.13.4.2 Các kết quả của giai đoạn này phải được ghi lại, cùng với mọi giả thiết và các chứng minh được thực hiện trong suốt giai đoạn.

6.13.4.3 Duy trì việc ghi lại cả các nhiệm vụ thẩm tra, xác nhận và chấp nhận được tiến hành trong giai đoạn.

6.13.4.4 Nên tạo ra một Sổ tay nguy hiểm được cập nhật trong giai đoạn này.

6.13.4.5 Phải tạo ra một Hồ sơ an toàn ứng dụng cập nhật trong giai đoạn này.

6.13.4.6 Tất cả các tài liệu liên quan tới RAM nên được xem xét lại và cập nhật khi cần thiết.

6.13.4.7 Các tài liệu chuyển giao của giai đoạn này là đầu vào chính cho các giai đoạn vòng đời hệ thống sau này.

6.13.5 Thẩm tra

Các nhiệm vụ thẩm tra quy trình dưới đây phải được tiến hành trong giai đoạn này:

a) Đánh giá sự phù hợp của thông tin và khi cần thiết là dữ liệu và các thống kê khác, được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này;

b) Thẩm tra và xác nhận mọi thay đổi hoặc hiệu chỉnh đối với hệ thống có phù hợp với các yêu cầu RAMS đối với hệ thống và các yêu cầu chi phí vòng đời hệ thống;

c) Đánh giá sự phù hợp và mức độ hoàn thiện của mọi tài liệu hệ thống được bổ sung, đặc biệt là mọi hồ sơ an toàn hệ thống;

d) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn;

e) Đánh giá năng lực của tất cả các cá nhân thực hiện nhiệm vụ trong giai đoạn.

6.14 Giai đoạn 14: Ngừng hoạt động và hủy bỏ

6.14.1 Mục tiêu

Mục tiêu của giai đoạn này là phải kiểm soát được các nhiệm vụ ngừng hoạt động và hủy bỏ.

6.14.2 Các đầu vào

Đầu vào cho giai đoạn này phải bao gồm tất cả các thông tin liên quan và khi phù hợp là dữ liệu cần thiết để đáp ứng yêu cầu.

6.14.3 Các yêu cầu

6.14.3.1 Yêu cầu 1 của giai đoạn này là phải:

a) Thiết lập tác động của việc ngừng hoạt động và hủy bỏ lên mọi hệ thống hoặc các yếu tố bên ngoài liên quan tới hệ thống bị ngừng hoạt động.

b) Lập kế hoạch ngừng hoạt động, bao gồm thiết lập các quy trình cho:

- Ngừng hệ thống an toàn và mọi yếu tố bên ngoài liên quan;
- Tháo dỡ hệ thống an toàn và các yếu tố bên ngoài liên quan;
- Tiếp tục đảm bảo sự phù hợp với các yêu cầu RAMS của mọi hệ thống hoặc các yêu tố bên ngoài bị tác động bởi sự ngừng hoạt động hệ thống.

6.14.3.2 Yêu cầu 2 của giai đoạn này là phải đưa ra một phân tích về đặc tính vòng đời hệ thống RAMS sử dụng cho các hệ thống tương lai, bao gồm cả dự toán chi phí về vòng đời hệ thống.

6.14.4 Tài liệu chuyển giao

6.14.4.1 Các kết quả của giai đoạn này phải được ghi lại, cùng với mọi giả thiết và các minh chứng được thực hiện trong suốt giai đoạn.

6.14.4.2 Phải duy trì việc ghi lại tất cả các nhiệm vụ ngừng hoạt động và hủy bỏ được tiến hành trong giai đoạn.

6.14.4.3 Nên tạo ra một Sổ tay nguy hiểm được cập nhật trong giai đoạn này.

6.14.4.4 Nên thiết lập kế hoạch an toàn để đề cập đến các nhiệm vụ ngừng hoạt động và hủy bỏ và được kết thúc sau khi hoàn thiện công việc.

6.14.4.5 Có thể tạo ra một Hồ sơ an toàn ứng dụng được sửa đổi trong giai đoạn này.

6.14.4.6 Có thể đưa ra tài liệu ghi chép được cập nhật giải quyết sự phù hợp sau đó với các yêu cầu về RAMS của các hệ thống liên quan bị tác động trong các nhiệm vụ ngừng hoạt động và hủy bỏ.

6.14.5 Thẩm tra

Phải tiến hành các nhiệm vụ thẩm tra quy trình trong giai đoạn này như sau:

a) Đánh giá sự phù hợp của thông tin và khi cần là dữ liệu và các thống kê khác, được sử dụng là đầu vào cho các nhiệm vụ trong giai đoạn này;

b) Đánh giá sự phù hợp của mọi ghi chép tài liệu đối với các hệ thống bị ảnh hưởng bởi các hoạt động ngừng hoạt động và hủy bỏ;

c) Đánh giá sự phù hợp của các phương pháp, các công cụ và các kĩ thuật được sử dụng trong giai đoạn;

d) Đánh giá năng lực của tất cả các cá nhân thực hiện các nhiệm vụ trong giai đoạn.

Phụ lục A

(tham khảo)

Ví dụ về quy định RAMS

A.1 Tổng quan

Để tạo điều kiện cho việc áp dụng tiêu chuẩn này, phụ lục này trình bày một ví dụ cơ bản chính về quy định RAMS đối với các hệ thống đường sắt. Ví dụ cơ bản này sẽ liên quan tới Hình 8 và Hình 9 của tiêu chuẩn và các mô tả tương ứng của các giai đoạn vòng đời hệ thống được nêu chi tiết trong điều 6, sử dụng phương tiện giao thông đường sắt là ví dụ để minh họa chi tiết trong ví dụ cơ bản này.

A.2 Cấu trúc

Cấu trúc và nội dung cơ bản của quy định RAMS (là một phần trong các yêu cầu tổng thể hệ thống) có thể dựa theo ví dụ cơ bản dưới đây:

1. Xác định hệ thống

1.1. Xác định dự án;

1.2. Sản phẩm chuyển giao và giới hạn về thời gian dự án;

1.3. Tổ chức dự án và Quản lý RAMS.

2. Mô tả chung về hệ thống

2.1. Mô tả kĩ thuật hệ thống;

2.2. Khai thác và vận hành cụ thể

Ví dụ: Đối với phương tiện giao thông đường sắt

- Vận hành đoàn tàu cao tốc;
- Các tổng thành của đoàn tàu;
- Hồ sơ nhiệm vụ;
- Vị trí địa lý;
- Kế hoạch chạy tàu và các sai số cho phép ;
- Chiến lược vận hành;

- Các nguyên tắc an toàn;
- Các xem xét về yếu tố con người.

2.3. Mô tả kĩ thuật các hệ thống con:

Ví dụ: Đối với phương tiện giao thông đường sắt:

- Hệ thống cung cấp năng lượng;
- Hệ thống hãm;
- Hệ thống kéo;
- Thông gió;
- Hệ thống bảo vệ;
- Hệ thống kiểm soát;
- Hệ thống liên lạc;
- Sưởi ấm.

3. Các điều kiện vận hành và môi trường

3.1. Xác định các chế độ vận hành:

Ví dụ: đối với phương tiện giao thông đường sắt:

- Thời gian vận hành hoặc quãng đường vận hành trong một ngày;
- Thời gian chờ trong một ngày;
- Thờ gian không vận hành trong một ngày;

3.2. Kỳ vọng tuổi thọ:

Ví dụ: đối với phương tiện giao thông đường sắt:

- Tổng thời gian được lập kế hoạch cho việc sử dụng hệ thống (năm);
- Thời gian vận hành trung bình một năm.

3.3. Xác định các điều kiện môi trường:

Ví dụ: đối với phương tiện giao thông đường sắt:

- Các tiêu chuẩn tuân theo;
- Dải nhiệt độ môi trường vận hành;
- Dải nhiệt độ của phương tiện;
- Khi đang vận hành;
- Khi không vận hành;
- Dải độ ẩm môi trường vận hành;
- Độ cao tối đa so với mực nước biển.

4. Độ tin cậy

4.1. Các mục tiêu về độ tin cậy:

4.2. Xác định các mục tiêu về độ tin cậy để đáp ứng sự hoạt động được yêu cầu của hệ thống đường sắt cụ thể (xem 2.2);

4.3. Các dạng hư hỏng hệ thống và Thời gian trung bình giữa các lần hư hỏng (MTBF):

Ví dụ: đối với phương tiện giao thông đường sắt:

Loại hư hỏng	Dạng hư hỏng hệ thống	Tác động đến vận hành	MTBF (.) *
Nghiêm trọng (Significant)	Hư hỏng toàn bộ	Không thể vận hành	
Lớn (Major)	Hư hỏng chức năng chính	Vận hành khẩn cấp 1	
Nhỏ (minor)	Hư hỏng chức năng phụ	Vận hành khẩn cấp 2	
Không đáng kể (Negligible)	Hư hỏng chức năng bình thường	Vận hành bình thường	

*. MTBF(.): tính bằng giờ, năm hoặc km.

Xem thêm mục 4.5.5.2, bảng 1 và phụ lục C, bảng C.1 để tham khảo.

4.4. Ảnh hưởng đến vận hành / sự hoạt động:

Ví dụ: đối với phương tiện giao thông đường sắt:

- Xác định các điều kiện kĩ thuật và vận hành của những bộ phận chính trong khai thác khi hư hỏng toàn bộ, vận hành khẩn cấp 1, vận hành khẩn cấp 2 và hư hỏng không ảnh hưởng đến vận hành;

Loại hư hỏng	Ảnh hưởng đến vận hành*	Hoạt động			Chú ý
		Nguồn (%)	Tốc độ (%)	(.)	
Nghiêm trọng (Significant)	Không thể vận hành	0	0		
Lớn (Major)	Vận hành khẩn cấp 1				
Nhỏ (minor)	Vận hành khẩn cấp 2				
Không đáng kể (Negligible)	Vận hành bình thường	100	100		Hiển thị thông tin được giảm bớt

*Xác định các điều kiện kĩ thuật và vận hành trong khai thác đối với:

- Hư hỏng toàn bộ;
- Vận hành khẩn cấp 1;
- Vận hành khẩn cấp 2;
- Hư hỏng không ảnh hưởng đến vận hành

5. Bảo dưỡng và sửa chữa

5.1. Bảo dưỡng phòng ngừa:

Mô tả về chính sách bảo dưỡng và cấp sửa chữa R0-R3.

Ví dụ: đối với phương tiện giao thông đường sắt:

Cấp sửa chữa	MTBM	MTTM
R0		
R1		
R2		
R3		

MTBM: Thời gian trung bình giữa các lần bảo dưỡng (giờ, năm hoặc km)

MTTM: Thời gian trung bình bảo dưỡng (Thời gian trung bình của sửa chữa, giờ hoặc ngày)

Xem thêm tham khảo trong phụ lục C, bảng C.2 và bảng C.4

5.2. Sửa chữa:

Mô tả về chính sách sửa chữa và nguồn lực cung ứng cần thiết

- Quy định MTTR (Thời gian trung bình để khôi phục) hệ thống (bằng giờ hoặc ngày);
- Xác định các thành phần thời gian có trong MTTR:
  - Thời gian điều động/di chuyển;
  - Thời gian tiếp cận;
  - Thời gian cung cấp các phụ tùng thay thế (hậu cần);
  - Thời gian sửa chữa/thay thế;
  - Thời gian thử nghiệm/khởi động;
  - Thời gian thu thập dữ liệu;
  - Thời gian chờ đợi.
- Quy định thời gian sửa chữa / thay thế và các điều kiện của từng hạng mục có thể sửa chữa được (các thời gian sửa chữa/thay thế tối đa hoặc trung bình);
- Quy định khả năng cung ứng tối thiểu của các phụ tùng thay thế và các điều kiện nguồn lực cung ứng;

Ví dụ:

Các bộ phận có thể sửa chữa	Thời gian sửa chữa thay thế trung bình	Địa điểm sửa chữa	Số lượng công nhân sửa chữa cần thiết

6. Độ an toàn

6.1. Các mục tiêu về an toàn:

- Mô tả các mục tiêu an toàn và chính sách áp dụng (xem mục 2.2).

6.2. Các điều kiện nguy hiểm:

- Xác định và liệt kê các nguy hiểm được xem xét trong khai thác;

- Quy định các mức độ xác suất nguy hiểm (xem 4.6.2.2, Bảng 2).

6.3. Các chức năng và hư hỏng liên quan tới an toàn:

- Xác định và liệt kê các chức năng liên quan tới an toàn, ví dụ: quá trình hãm hoặc các thiết bị hãm);

- Quy định các hư hỏng liên quan tới an toàn trong hệ thống đối với từng chức năng liên quan tới an toàn (xem mục 4.3.6 và 4.3.7):

Ví du: Phương tiện giao thông đường sắt

Chức năng/bộ phận liên quan tới an toàn	Đặc điểm của hư hỏng liên quan tới an toàn	MTBSF* (năm hoặc km)
Hãm		
Cửa toa xe khách		

*Xem phụ lục C, Bảng C.5

- Các mức độ nghiêm trọng của nguy hiểm về an toàn;

- Xác định các mức độ nghiêm trọng của nguy hiểm về an toàn có thể áp dụng (xem 4.6.2.3, Bảng 3);

- Phân loại rủi ro;

- Xác định khả năng chấp nhận được cho các rủi ro (xem 4.6.3.2 và 4.6.3.3).

7. Tính sẵn sàng

Tính sẵn sàng hệ thống A có thể được quy định thành các phần:

- Tính không sẵn sàng được lập kế hoạch (bảo dưỡng): 1 - AM

- Tính không sẵn sàng không được lập kế hoạch (sửa chữa): 1 - AR

- $A = 1 – [(1 - AM) + (1 – AR)]$

- $A = MUT/(MUT + MDT); 0 \leq A \leq 1$

- Trong đó

- MUT = Thời gian sử dụng trung bình, thay thế phù hợp cho MTBF, MTBSF…

- MDT = Thời gian không sử dụng trung bình, thay thế phù hợp cho MTTM, MTTR…

- MUT và MDT được xác định đối với Tính sẵn sàng cụ thể A (.)

- Ví dụ: Đối với tính sẵn sàng AS của “hệ thống an toàn” (MUT=MTBSF).

- Thời gian down d(T) theo thời gian thực hiện nhiệm vụ T (ví dụ: 1 năm) tính ra là:

$$d(T) = (1 – A) * T$$

7.1. Quy định tính sẵn sàng:

- Quy định tính sẵn sàng hệ thống A đi kèm với các yêu cầu về bảo dưỡng và sửa chữa (mục 5);

- Chính sách bảo dưỡng và sửa chữa phải được tuyên bố, dựa trên tính sẵn sàng A.

8. Chứng minh đặc tính RAMS.

Xác định việc chứng minh đặc tính RAMS được trình bày trong giai đoạn 9 - Xác nhận hệ thống và giai đoạn 10 - Chấp nhận hệ thống.

Chứng minh đặc tính RAMS được thực hiện qua việc đưa ra các bằng chứng như:

- Quản lý và tổ chức RAMS;

- Tính sẵn sàng của các nguồn lực RAMS;

- Quy định các yêu cầu về RAMS;

- Các kế hoạch và chương trình RAMS;

- Báo cáo xem xét liên quan tới RAMS;

- Báo cáo phân tích RAMS;

- Biên bản thử nghiệm RAMS (từng phần);

- Thu thập dữ liệu về hư hỏng (Thống kê);

- Hồ sơ an toàn ứng dụng cụ thể;

- Xác nhận và chấp nhận hệ thống;
- Giám sát đặc tính RAMS trong giai đoạn vận hành ban đầu;
- Đánh giá chi phí vòng đời hệ thống.

9. Chương trình RAMS

Đơn vị cung cấp được cho là ảnh hưởng lớn nhất tới sự đạt được các yêu cầu về RAMS cho dự án phải đưa ra Chương trình RAM và Kế hoạch an toàn.

Ví dụ về chương trình RAMS cơ bản được trình bày trong phụ lục B.

Phụ lục B

(Tham khảo)

Ví dụ về chương trình RAMS cơ bản

B.1 Phụ lục này đưa ra ví dụ về quy trình cơ bản cho một chương trình/kế hoạch an toàn RAM cơ bản và trình bày ví dụ về một chương trình RAMS cơ bản (Chương trình/Kế hoạch an toàn RAM). Đồng thời cũng liệt kê một số phương pháp và công cụ để quản lý và phân tích RAMS.

B.2 Đơn vị cung ứng nên thiết lập một Chương trình RAMS tạo điều kiện thuận lợi hiệu quả cho việc đáp ứng các yêu cầu về RAMS của hệ thống đường sắt được xem xét. Các chương trình RAMS của những dự án tương tự hoặc các yêu cầu hệ thống của đơn vị cung ứng có thể tạo ra một "chương trình RAMS tiêu chuẩn" thiết lập nên "RAMS-cơ bản" cho đơn vị.

B.3 Quy trình:

Quy trình ví dụ về Chương trình RAMS cơ bản được đưa ra dưới đây:

1. Xác định vòng đời hệ thống phù hợp cùng với quá trình kinh doanh của đơn vị.

   Kết quả: Thiết lập được vòng đời hệ thống của đơn vị hoặc các giai đoạn của dự án.

2. Chỉ định cho từng giai đoạn của dự án các đặc tính RAMS liên quan trong giai đoạn và các nhiệm vụ an toàn cần thiết để đáp ứng một cách đáng tin cậy các yêu cầu cụ thể của dự án và hệ thống.

   Kết quả: Xác định được tất cả các nhiệm vụ RAMS cần thiết trong vòng đời hệ thống.

3. Xác định các trách nhiệm trong đơn vị để thực hiện từng nhiệm vụ RAMS.

   Kết quả: Xác định nhân viên chịu trách nhiệm và các nguồn lực về RAMS cần thiết.

4. Xác định các chỉ dẫn, các công cụ và các tài liệu tham khảo cần thiết cho từng nhiệm vụ RAMS.

   Kết quả: Quản lý RAMS được lưu giữ lại.

5. Các hoạt động về RAMS được thực hiện trong các quá trình hoạt động của công ty.

   Kết quả: quá trình quản lý RAMS được tích hợp vào trong quá trình hoạt động (RAMS-cơ sở).

B.4 Ví dụ về chương trình RAMS cơ bản:

Một dạng cơ bản về chương trình RAMS cơ bản được đưa ra trong bảng B.1. Dạng cơ bản này bao gồm ví dụ về một loạt các nhiệm vụ có thể được áp dụng cho một dự án riêng.

Bảng B.1 – Ví dụ về một chương trình RAMS cơ bản

Dự án – giai đoạn	Các nhiệm vụ RAMS	Trách nhiệm	Tài liệu tham chiếu
Thu thập dữ liệu ban đầu	Đánh giá các mục tiêu về RAMS của hệ thống đường sắt cụ thể		
Nghiên cứu khả thi	- Đánh giá các yêu cầu về RAMS - Đánh giá dữ liệu và kinh nghiệm trước đây về RAMS - Xác định các ảnh hưởng đến an toàn phát sinh bởi hệ thống đường sắt cụ thể - Tư vấn khách hàng về RAMS (nếu cần thiết)		
Mời thầu	- Tiến hành phân tích RAMS sơ bộ (trường hợp xấu nhất) - Phân bổ các yêu cầu về RAMS hệ thống (Các hệ thống con / trang thiết bị, các hệ thống liên quan khác…) - Tiến hành phân tích nguy hiểm & rủi ro về an toàn hệ thống - Tiến hành phân tích rủi ro liên quan tới RAM - Chuẩn bị cho đánh giá dữ liệu RAMS tương lai - Các đánh giá theo từng mục trong hồ sơ mời thầu liên quan tới RAMS		
Đàm phán hợp đồng	- Xem xét/cập nhật phân tích RAMS sơ bộ và các phân bổ về RAMS		
Xử lý theo trình tự: Xác định các yêu cầu của hệ thống	- Thiết lập quản lý RAMS cụ thể cho dự án - Quy định các yêu cầu RAMS hệ thống (tổng thể) - Thiết lập chương trình RAMS (Chương trình RAMS tiêu chuẩn có đầy đủ?) - Chỉ định các yêu cầu RAMS cho các nhà thầu phụ, đơn vị cung ứng - Xác định chỉ tiêu chấp nhận RAMS (tổng thể)		
Xử lý theo trình tự: Thiết kế và thi công	- Phân tích độ tin cậy (FMEA) - Phân tích an toàn (FMECA), nếu có thể áp dụng - Phân tích bảo dưỡng/sửa chữa; xác định chính sách bảo dưỡng/sửa chữa - Phân tích tính sẵn sàng dựa trên chính sách bảo dưỡng/sửa chữa - Đánh giá chi phí vòng đời hệ thống		

Dự án – giai đoạn	Các nhiệm vụ RAMS	Trách nhiệm	Tài liệu tham chiếu
	- Thuyết minh RAMS, sự phù hợp các bằng chứng - Phân tích FMEA thiết kế/sản xuất - Thử nghiệm độ tin cậy và khả năng bảo dưỡng, nếu có thể áp dụng được		
Kết quả đạt được	- Đưa ra quy định về RAMS cho các nhà thầu phụ / đơn vị cung ứng		
Sản xuất / thử nghiệm	- Đảm bảo chất lượng / đảm bảo quá trình liên quan tới RAMS		
Thử hoạt động / chấp nhận	- Tiến hành chứng minh RAM - Chuẩn bị Hồ sơ an toàn ứng dụng cụ thể - Triển khai đánh giá dữ liệu về RAMS - Thử nghiệm RAM trong giai đoạn vận hành đầu tiên, sàng lọc và đánh giá dữ liệu		
Vận hành / bảo dưỡng	- Vận hành và bảo dưỡng theo quy định (chính sách bảo dưỡng / sửa chữa) - Đào tạo nhân lực vận hành và bảo dưỡng - Đánh giá dữ liệu về RAMS - Đánh giá chi phí vòng đời hệ thống - Đánh giá, xem xét sự hoạt động		

B.5 Danh sách các công cụ:

Một số phương pháp và công cụ phù hợp cho việc kiểm soát và quản lý một chương trình RAMS được liệt kê dưới đây. Việc lựa chọn công cụ liên quan sẽ dựa trên hệ thống được xem xét và tính quan trọng, độ phức tạp, tính mới lạ… của hệ thống.

1. **Dạng cơ bản về quy định RAMS:** để đảm bảo việc đánh giá các yêu cầu về RAMS liên quan (xem phụ lục A)

2. **Các quy trình để đánh giá thiết kế chính thức:** nhấn mạnh về RAMS, sử dụng một số các danh sách kiểm tra chung và ứng dụng riêng cho phù hợp…

IEC 61160 Xem xét thiết kế chính thức (Bổ sung lần 1)

3. **Quy trình để tiến hành phân tích RAM sơ bộ "từ trên xuống" (các phương pháp suy diễn) và "từ dưới lên" (phương pháp quy nạp), phân tích RAM của trường hợp xấu nhất và theo chiều sâu đối với các kết cấu hệ thống chức năng phức tạp và đơn giản:** tổng quan về các quy trình, các

phương pháp phân tích RAM được sử dụng phổ biến, ưu điểm, nhược điểm, đầu vào dữ liệu và các yêu cầu khác đối với các kĩ thuật khác nhau được đưa ra trong:

IEC 60300-3-1	Quản lý độ tin cậy – Phần 3: - Hướng dẫn áp dụng – Mục 1: Kĩ thuật phân tích độ tin cậy: Hướng dẫn về phương pháp

Các kĩ thuật phân tích RAM khác nhau được mô tả trong các tiêu chuẩn riêng, một số như dưới đây:

IEC 600706	Hướng dẫn về bảo dưỡng thiết bị
IEC 600706-1	Phần 1: Mục 1, 2 và 3: Giới thiệu, các yêu cầu và chương trình bảo dưỡng
IEC 600706-2	Phần 2 – Mục 5: Các nghiên cứu về khả năng bảo dưỡng trong suốt giai đoạn thiết kế
IEC 600706-3	Phần 3 – Mục 6 và 7: Thẩm tra và thu thập, phân tích và trình bày dữ liệu
IEC 600706-4	Phần 4 – Mục 8: Bảo dưỡng và lập kế hoạch hỗ trợ bảo dưỡng
IEC 600706-5	Phần 5 – Mục 4: Thử nghiệm xử lý sự cố
IEC 600706-6	Phần 6 – Mục 9: Các phương pháp thống kê trong quá trình đánh giá khả năng bảo dưỡng
IEC 60812	Kĩ thuật phân tích độ tin cậy hệ thống – Quy trình phân tích dạng hư hỏng và hậu quả (FMEA)
IEC 60863	Thể hiện các dự báo về độ tin cậy, tính sẵn sàng và khả năng bảo dưỡng
IEC 61025	Phân tích sự cố hình cây (FTA)
IEC 61078	Kĩ thuật phân tích tính phụ thuộc – phương pháp sơ đồ khối độ tin cậy
IEC 61165	Áp dụng kĩ thuật Markov

Tính sẵn sàng của dữ liệu “RAM” thống kê mang tính hỗ trợ, đối với các tổng thành được sử dụng trong thiết kế (thông thường: cường độ hư hỏng, tỷ lệ sửa chữa, dữ liệu bảo dưỡng, các dạng hư hỏng, tỷ lệ tình huống, phân chia dữ liệu và các tình hống ngẫu nhiên…) là cơ bản để phân tích RAM…

IEC 61709	Các thiết bị điện tử - Độ tin cậy – Các điều kiện tham chiếu về các dạng áp lực tạo ra hư hỏng để đánh giá tỷ lệ phá hoại
US MIL HDBK 217	Dự đoán độ tin cậy cho các hệ thống điện tử

Đồng thời cũng phải có một số các chương trình máy tính để phân tích RAM hệ thống và phân tích dữ liệu thống kê.

4. **Quy trình để tiến hành phân tích nguy hiểm và an toàn/rủi ro.** Một số được mô tả trong:

US ML HDBK 882C	Các yêu cầu về chương trình an toàn hệ thống
US MIL HDBK 764 (MI)	Kĩ thuật an toàn hệ thống, hướng dẫn thiết kế đối với vật liệu quốc phòng.

Kĩ thuật cơ bản và các phương pháp phân tích giống nhau được liệt kê cho RAM (mục 3), cũng có thể áp dụng được cho phân tích an toàn/rủi ro

Xem IEC 61508, Phần 1-7, dưới tiêu đề chung "An toàn chức năng của các hệ thống liên quan tới an toàn điện tử của điện/điện tử/điện tử lập trình", bao gồm những phần sau:

- Phần 1: Các yêu cầu chung;
- Phần 2: Các yêu cầu cho các hệ thống điện điện tử/điện/lập trình;
- Phần 3: Các yêu cầu phần mềm;
- Phần 4: Định nghĩa và viết tắt;
- Phần 5: Ví dụ về phương pháp xác định mức toàn vẹn về an toàn;
- Phần 6: Hướng dẫn về áp dụng phần 2 và 3;
- Phần 7: Tổng quan về các kĩ thuật và biện pháp.

5. **Kế hoạch và quy trình thử nghiệm RAMS:** để thử nghiệm tính năng vận hành trong thời gian dài của các tổng thành, thiết bị hoặc các hệ thống và để chứng minh nó thỏa mãn các yêu cầu. Ngoài ra, phân tích RAMS và các kết quả thử nghiệm còn được sử dụng để tạo ra các chương trình cải tiến RAMS.

IEC 60605	Thử nghiệm độ tin cậy của thiết bị
IEC 60605-1 + A1	Phần 1: Các yêu cầu chung
IEC 60605-2	Phần 2: Thiết kế vòng đời hệ thống thử nghiệm
IEC 60605-3-1	Phần 3: Các điều kiện thử nghiệm ưu tiên. Thiết bị di động trong nhà – Mô phỏng mức độ thấp
IEC 60605-3-2	Phần 3: Các điều kiện thử nghiệm ưu tiên –Thiết bị sử dụng tĩnh ở các vị trí được bảo vệ khỏi thời tiết – Mô phỏng mức độ cao

IEC 60605-3-3	Phần 3: Các điều kiện thử nghiệm ưu tiên – Mục 3: Chu trình thử nghiệm 3: Thiết bị sử dụng tĩnh ở các vị trí được bảo vệ khỏi thời tiết – Mô phỏng mức độ thấp
IEC 60605-3-4	Phần 3: các điều kiện thử nghiệm ưu tiên – Mục 4: vòng đời hệ thống thử nghiệm 4: Thiết bị sử dụng tĩnh và di động – Mô phỏng mức độ thấp
IEC 60605-4 + A1	Phần 4: Quy trình xác định các đánh giá điểm và các giới hạn độ tin cậy để thử nghiệm xác định độ tin cậy thiết bị
IEC 60605-6	Phần 6: Các thử nghiệm xác nhận tỉ suất hư hỏng cố định hoặc các giả thiết cường độ hư hỏng cố định
IEC 61014	Các chương trình gia tăng độ tin cậy
IEC 61070	Quy trình thử nghiệm thỏa mãn tính sẵn sàng không đổi
IEC 61123	Thử nghiệm độ tin cậy – Kế hoạch thử nghiệm sự phù hợp đối với tỉ suất thành công

Quan trọng hơn là **việc đánh giá dữ liệu RAMS từ mảng dữ liệu** (Thử nghiệm RAMS trong quá trình vận hành…), ví dụ:

IEC 60300-3-2	Quản lý độ tin cậy – Phần 3: hướng dẫn áp dụng – Phần 2: dữ liệu độ tin cậy từ mảng dữ liệu
IEC 60319	Thể hiện dữ liệu độ tin cậy trên các thiết bị điện tử (hoặc các bộ phận)

6. Quy trình/công cụ để tiến hành phân tích LCC (chi phí vòng đời hệ thống): có sẵn các chương trình máy tính khác nhau để phân tích LCC

Phụ lục C

(tham khảo)

Ví dụ về các thông số đường sắt

Ví dụ về các thông số và ký hiệu thông thường, phù hợp để sử dụng trong khai thác đường sắt:

C.1 Thông số độ tin cậy

Bảng C.1 – Ví dụ về các thông số độ tin cậy

Thông số	Ký hiệu	Đơn vị
Cường độ hư hỏng	Z(t), λ	Hư hỏng/thời gian, quãng đường, vòng đời hệ thống
Thời gian sử dụng trung bình	MUT	Thời gian, quãng đường, vòng đời hệ thống
Thời gian trung bình dẫn đến hư hỏng Quãng đường vận hành trung bình dẫn đến hư hỏng (đối với các hạng mục không thể sửa chữa)	MTTF MDTF	Thời gian, quãng đường, vòng đời hệ thống
Thời gian trung bình giữa các lần hư hỏng Quãng đường vận hành giữa các lần hư hỏng (Đối với các hạng mục sửa chữa được)	MTBF MDBF	Thời gian, quãng đường, vòng đời hệ thống
Xác suất hư hỏng	F(t)	Không có đơn vị
Độ tin cậy (xác suất không hỏng)	R(t)	Không có đơn vị

C.2 Các thông số về khả năng bảo dưỡng

Bảng C.2 – Ví dụ về các thông số khả năng bảo dưỡng

Thông số	Ký hiệu	Đơn vị
Thời gian không sử dụng trung bình	MDT	Thời gian, quãng đường, vòng đời hệ thống
Thời gian/ Quãng đường trung bình giữa các lần bảo dưỡng	MTBM/MDBM	Thời gian, quãng đường, vòng đời hệ thống
MTBM/MDBM, sửa chữa hoặc phòng	MTBM(c)/MDBM(c),	Thời gian, quãng đường, vòng

ngừa	MTBM(p)/MDBM(p)	đời hệ thống
Thời gian trung bình để bảo dưỡng	MTTM	Thời gian
MTTM, sửa chữa hoặc phòng ngừa	MTTM(c), MTTM(p)	Thời gian
Thời gian trung bình để khôi phục	MTTR	Thời gian
Tỷ lệ báo hỏng	FAR	Thời gian^{-1}
Phạm vi hư hỏng	FC	Không có đơn vị
Phạm vi sửa chữa	RC	Không có đơn vị

C.3 Các thông số tính sẵn sàng

Bảng C.3 – Ví dụ về các thông số tính sẵn sàng

Thông số	Ký hiệu	Đơn vị
Tính sẵn sàng Vốn có Đạt được Sử dụng	A (.) = MUT/(MUT+MDT) A i A a A o	Không có đơn vị
Tính sẵn sàng của đoàn xe	FA (= các phương tiện sẵn sàng / đoàn xe)	Không có đơn vị
Khả năng duy trì kế hoạch	SA	Không có đơn vị

C.4 Thông số nguồn lực cung ứng

Bảng C.4 – Ví dụ về thông số nguồn lực cung ứng

Thông số	Ký hiệu	Đơn vị
Chi phí vận hành và bảo dưỡng	O&MC	Tiền
Chi phí bảo dưỡng	MC	Tiền
Giờ công bảo dưỡng	MMH	Thời gian (giờ)
Độ trễ vật tư và quản lý	LAD	Thời gian
Thời gian sửa chữa sự cố		Thời gian
Thời gian sửa chữa		Thời gian

Hoạt động hỗ trợ bảo dưỡng		Không có đơn vị
Nhân lực cho việc thay thế	EFR	Không có đơn vị
Xác suất các phụ tùng thay thế trên thị trường khi cần	SPS	Không có đơn vị

C.5 Thông số về độ an toàn

Bảng C.5 – Ví dụ về các thông số hoạt động an toàn

Thông số	Ký hiệu	Đơn vị
Thời gian trung bình giữa các lần hư hỏng nguy hiểm	MTBF(H)	Thời gian, quãng đường, vòng đời hệ thống
Thời gian trung bình giữa các lần "hư hỏng an toàn hệ thống"	MTBSF	Thời gian, quãng đường, vòng đời hệ thống
Tỷ lệ nguy hiểm	H(t)	Hư hỏng/thời gian, quãng đường, vòng đời hệ thống
Xác suất hư hỏng liên quan tới an toàn	$F_s(t)$	Không có đơn vị
Xác suất an toàn chức năng	$S_s(t)$	Không có đơn vị
Thời gian để trở về trạng thái an toàn	TTRS	Thời gian

Phụ lục D

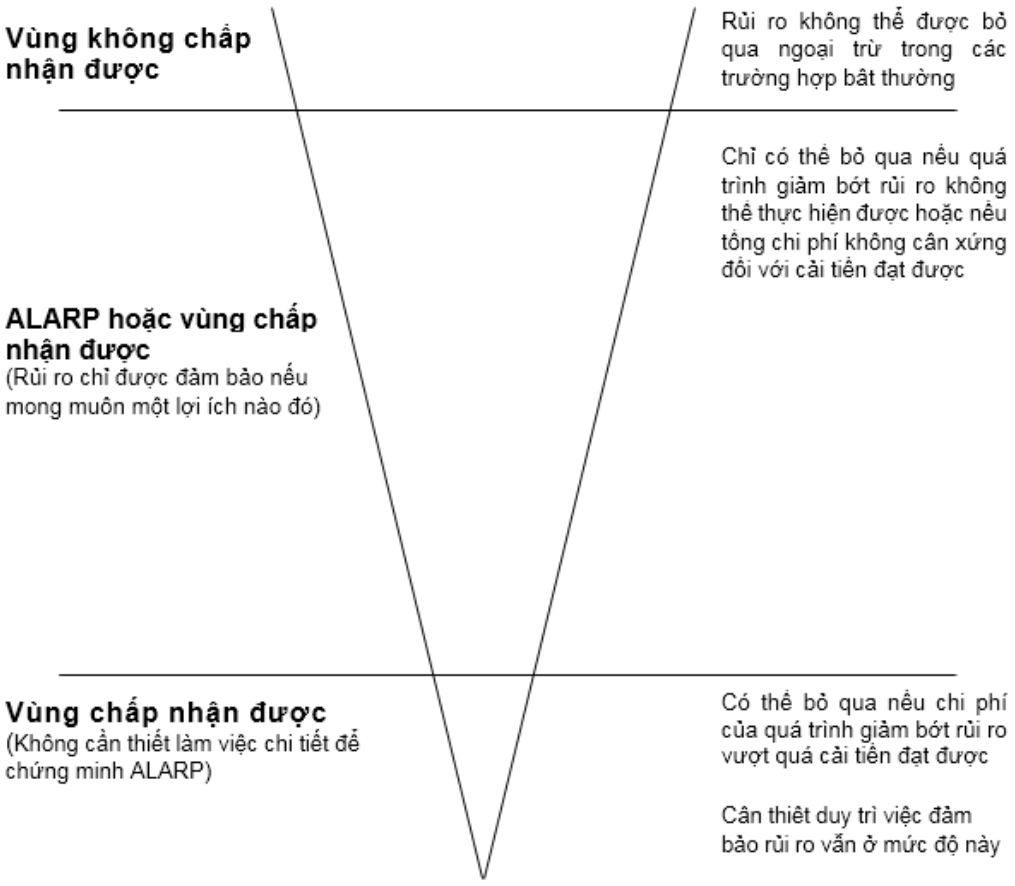
(Tham khảo)

Ví dụ về một số nguyên tắc chấp nhận rủi ro

CHÚ THÍCH: Các giá trị được đưa ra trong phụ lục này chỉ có tác dụng minh họa nguyên tắc và không có ý định sử dụng cho các mục đích khác

D.1 Nguyên tắc Thấp đến mức có thể thực hiện được một cách hợp lý (ALARP)

Nguyên tắc có thể được thể hiện bằng sơ đồ như dưới đây:



Hình D.1 – Nguyên tắc ALARP

D.1.1 Một số rủi ro là quá lớn và một số kết quả không thể chấp nhận được nên chúng không thể bị bỏ qua và không thể chứng minh trên mọi phương diện. Giới hạn trên của sơ đồ xác định các mức độ rủi ro không thể chấp nhận được. Nếu mức rủi ro không thể bị giảm bớt dưới đường biên này thì quá trình vận hành không thể thực hiện được.

D.1.2 Giới hạn dưới của sơ đồ xác định vùng chấp nhận được khi các rủi ro được xem là quá thấp, từ đó các hoạt động giảm thêm sẽ không có khả năng minh chứng bằng mọi chỉ số ALARP.

D.1.3 Vùng nằm giữa giới hạn trên và dưới được gọi là vùng ALARP. Phải khẳng định rằng không thể chứng minh đầy đủ việc các rủi ro là nằm trong vùng ALARP. Chúng phải được làm cho thấp đến mức có thể được thực hiện hợp lý. Có nhiều cách để chứng minh ALARP. Có thể đưa ra đầy đủ các tiêu chuẩn và áp dụng thực tế hiện tại sẵn có tốt nhất có thể đang được áp dụng. Đối với các vận hành lần đầu (mới), hoặc khi tính đầy đủ của các tiêu chuẩn và áp dụng thực tế hiện tại là đang nghi vấn, các khái niệm về phân tích lợi ích chi phí và giá trị của sự tồn tại có thể được đưa ra.

D.1.4 Rủi ro xã hội phải được kiểm tra khi có khả năng về thảm họa liên quan tới số lượng lớn các tử vong. Việc không chấp nhận số lượng lớn các tai nạn được gọi là “Sự không mong muốn rủi ro khác nhau” (DRA). Giá trị này được thể hiện bằng độ dốc (-1) của đường cong log F-N, trong đó F là tần suất xuất hiện (năm^{-1}) và N là số lượng tử vong trong một lần xuất hiện.

D.2 Nguyên tắc rủi ro tổng thể càng thấp càng tốt (GAMAB)

Công thức hoàn chỉnh của nguyên tắc này như sau:

“Tất cả các hệ thống giao thông dẫn hướng mới phải đưa ra mức độ rủi ro tổng thể ít nhất bằng mức độ rủi ro đã được chỉ định cho bất kì một hệ thống tương đương hiện tại”

D.2.1 Công thức này tính tới những công việc đã được thực hiện và yêu cầu một cách hàm ý quá trình phải được thực hiện trong hệ thống được lập dự án, bằng yêu cầu “ít nhất”. Không xem xét rủi ro cụ thể, bằng yêu cầu “tổng thể”. Bên cung cấp hệ thống giao thông được tự do phân chia các rủi ro khác nhau sẵn có trong hệ thống và áp dụng các cách tiếp cận liên quan, ví dụ: định tính hoặc định lượng.

D.2.2 Khi sử dụng cách định lượng, có thể chuyển thành phương pháp sau:

1. Gọi $\tau_{c.\mathrm{ref}}$ là tỉ lệ (tử vong/hành khách) lấy từ số lượng xác định các hành khách được vận chuyển bởi một hệ thống giao thông trong những năm vận hành trước đây và các tử vong gây ra do va chạm giữa 2 đoàn tàu. Tỉ lệ này rút ra từ các thống kê cho các hệ thống đang tồn tại và là chỉ tiêu tham chiếu cho hệ thống mới, có cùng đặc tính.

2. Xem xét hệ thống mới (thay thế). Từ hệ thống mới này, gọi:

C = Năng lực vận chuyển của đoàn tàu (số hành khách/đoàn tàu)

F = Tần suất của đoàn tàu (số đoàn tàu/giờ)

r = Hệ số chiếm dụng trung bình (đoàn tàu không hoàn toàn đầy)

n_C = Số lượng tử vong trong mỗi vụ va chạm trong hệ thống mới này

D_m = Lưu lượng thông qua (số hành khách/giờ) = r * C * F.

Từ đó, số lượng các va chạm thực tế cho từng hành khách (col) là:

$Col = (\tau_{C.\text{ref}} / n_c)$. (va chạm/hành khách)

Đồng thời, tỷ lệ va chạm cho hệ thống mới phải nhỏ hơn tỷ lệ của hệ thống đã có:

Từ đó:

$\lambda_C \le col.D_M = (\tau_{C.\text{ref}} / n_c).D_M = \tau_{C.\text{ref}}.(r.C / n_C).F$ va chạm/giờ

3. Chú ý

Giả thiết rằng số các tử vong giữa các hành khách trong cùng một đoàn tàu là giống nhau giữa hệ thống đã có và hệ thống được lập dự án:

- Ví dụ: n_C/r.C = không đổi;

- λ_C có thể là yêu cầu khó đối với khai thác chất lượng thấp, đặc biệt giá trị F thấp (tần suất đoàn tàu);

- Cải tiến được thể hiện bằng dấu ≤

- Bên cung cấp/thiết kế tự do phân chia trị số λ_C giữa thiết bị bên đường và thiết bị trên tàu.

D.3 Nguyên tắc tỉ lệ tử vong nội sinh nhỏ nhất (MEM)

Nguyên tắc này phát sinh từ vấn đề dưới đây:

1. Chết người có nhiều nguyên nhân khác nhau. Một nhóm các nguyên nhân được gọi là “các yếu tố kĩ thuật”, ví dụ:

- Giải trí và thể thao;

- Làm các hoạt động tự bản thân;

- Làm công việc máy móc;

- Vận chuyển.

Không có những nguyên nhân dưới đây:

- Chết do bệnh tật hoặc ốm;

- Chết do dị tật bẩm sinh.

Nhóm này tạo ra tỉ lệ phần trăm nhất định người chết trên từng năm, tỷ lệ này thay đổi theo tuổi thọ dân số được xét. Rủi ro này được gọi là "Tỉ lệ tử vong nội sinh" "R".

2. Ở các đất nước phát triển, R là thấp nhất đối với nhóm tuổi từ 5 đến 15. Mức thấp nhất này của Tỉ lệ tử vong nội sinh, gọi là "Tỷ lệ tử vong nội sinh nhỏ nhất" R_m tính bằng:

$R_m = 2.10^{-4}$ tử vong/người.năm

3. Từ đó, hình thành nguyên tắc sau:

"Các nguy hiểm tạo ra từ hệ thống giao thông mới sẽ không làm tăng đáng kể đại lượng R_m".

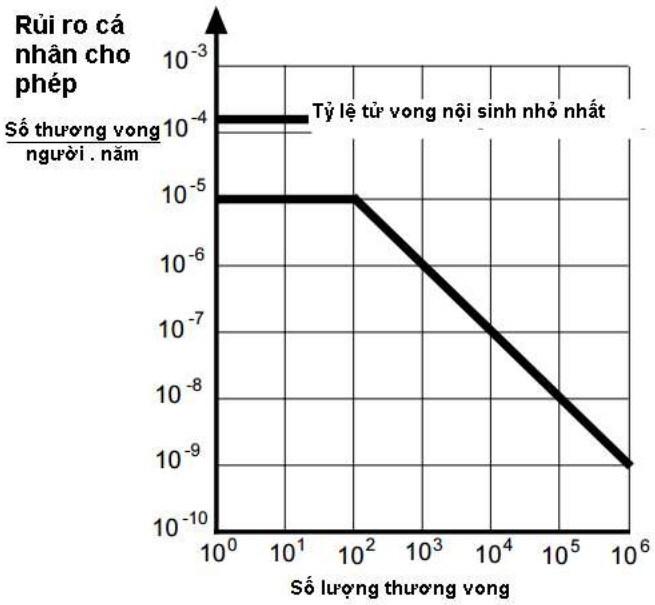
Trong thực tế, các chỉ số sau có thể được sử dụng:

$R_1 \leq 10^{-5}$ tử vong/người.năm

$R_2 \leq 10^{-4}$ thương nặng/người.năm

$R_3 \leq 10^{-3}$ thương nhẹ/người.năm

Quan điểm này mang tính cá nhân cao: gia đình của người chịu tử vong sẽ không tìm thấy được bất cứ sự an ủi nào khi thực tế người thân của họ phải chịu trong một thảm họa dù lớn hay nhỏ. Điều này sẽ còn đúng cho tới khi vẫn liên quan tới các phương tiện giao thông hiện nay (tàu, máy bay…). Đối với các hệ thống có thể gây ra số lượng tai nạn lớn, chỉ số "Sự không mong muốn rủi ro khác nhau" (DRA) được đưa ra bằng độ dốc đi xuống như được thể hiện trong đường cong dưới đây:


Rủi ro cá nhân cho phép
Số thương vong / người . năm
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10^{-9}
10^{-10}
Tỷ lệ tử vong nội sinh nhỏ nhất
10^{0} 10^{1} 10^{2} 10^{3} 10^{4} 10^{5} 10^{6}
Số lượng thương vong

Phụ lục E

(Tham khảo)

Trách nhiệm xử lý RAMS trong suốt vòng đời hệ thống

Như một hướng dẫn chung, đối với một dự án đường sắt điển hình, áp dụng những điều dưới đây:

- Các yêu cầu thường được thiết lập bởi khách hàng hoặc cơ quan quản lý nhà nước (luật pháp).

- Việc thẩm định và chấp nhận sẽ được thực hiện một cách đồng bộ bởi khách hàng hoặc cơ quan nhà nước có thẩm quyền.

- Các giải pháp, các kết quả của chúng và các thẩm tra thường phải được soạn thảo kỹ lưỡng hoặc được thực hiện bởi nhà thầu.

- Việc xác nhận thường được thực hiện kết hợp giữa các tổ chức, cá nhân.

Tuy nhiên, nguyên tắc chung này phụ thuộc vào mối quan hệ dựa trên hợp đồng và luật pháp giữa các bên liên quan.

Mặt khác, tiêu chuẩn này yêu cầu trong từng trường hợp các trách nhiệm của các nhiệm vụ trong các giai đoạn vòng đời hệ thống khác nhau phải được xác định và thỏa thuận. Bảng dưới đây đưa ra ví dụ về các trách nhiệm đối với một sắp xếp bố trí phổ biến.

	Khách hàng / đơn vị vận hành	Cơ quan chứng nhận	Nhà thầu (chính)	Nhà thầu phụ	Đơn vị cung ứng
Giai đoạn ý tưởng	X				
Xác định hệ thống & các điều kiện hệ thống đường sắt	X				
Phân tích rủi ro	X		X		
Các yêu cầu của hệ thống	X	(X)			
Phân chia các yêu cầu của hệ thống	(X)		X		
Thiết kế và thi công			X	(X)	
Chế tạo sản xuất			X	X	X
Lắp đặt			X	(X)	
Xác nhận hệ thống	X	X	X	(X)	
Chấp nhận hệ thống	X	X			
Vận hành và bảo dưỡng	X		(X)	(X)	
Giám sát hoạt động	X		(X)	(X)	
Thay đổi và cải tiến	X		X	X	

Ngừng hoạt động và hủy bỏ	X		(X)		

Trong đó:

X – Trách nhiệm và tham gia đầy đủ

(X) – Trách nhiệm cụ thể và/hoặc tham gia một phần (ví dụ: nhà thầu phụ hoặc có liên quan)