TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 7384-100 : 2004

ISO/TR 13849-100 : 2000

Xuất bản lần 1

AN TOÀN MÁY -
BỘ PHẬN AN TOÀN LIÊN QUAN CỦA HỆ THỐNG ĐIỀU KHIỂN
Phần 100: HƯỚNG DẪN SỬ DỤNG VÀ ỨNG DỤNG TCVN 7384-1

Safety of machinery -

Safety-related parts of control systems -

Part 100: Guidelines for the use and application of ISO 13849-1

HÀ NỘI - 2008

Lời nói đầu

TCVN 7384-100:2004 tương đương với tiêu chuẩn ISO/TR 13849-100:2000 với những thay đổi biên tập cho phép.

TCVN 7384-100:2004 do Ban kỹ thuật tiêu chuẩn TCVN/SC 1 Những vấn đề chung về cơ khí biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ ban hành.

Tiêu chuẩn này được chuyển đổi năm 2008 Từ Tiêu chuẩn Việt Nam cùng số hiệu thành Tiêu chuẩn Quốc gia theo quy định tại khoản 1 Điều 69 của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật và điểm a khoản 1 Điều 6 Nghị định số 127/2007/NĐ-CP ngày 1/8/2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật.

An toàn máy - Bộ phận an toàn liên quan của hệ thống điều khiển - Phần 100: Hướng dẫn sử dụng và ứng dụng TCVN 7384-1:2004

Safety of machinery - Safety-related parts of control systems - Part 100: Guidelines for the use and application of ISO 13849-1

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra hướng dẫn sử dụng thích hợp và giải thích TCVN 7384-1:2004. Tiêu chuẩn này còn cung cấp thông tin thêm về các chủ đề sau:

- hệ thống điều khiển góp phần vào việc giảm rủi ro trong máy đến mức nào;
- tầm quan trọng của các bộ phận an toàn liên quan của hệ thống điều khiển đối với các chức năng an toàn như thế nào;
- lựa chọn và sử dụng đúng các loại;
- vai trò phụ lục B của TCVN 7384-1:2004.

2 Sử dụng đúng TCVN 7384-1:2004

Các vấn đề được giới thiệu trong TCVN 7384-1:2004 khá phức tạp. Các điều khoản của tiêu chuẩn liên quan với nhau và không thể sử dụng riêng một mình được. Do đó cần quan tâm đến tất cả các điều của TCVN 7384-1:2004.

3 Giải thích qui trình thiết kế

Qui trình thiết kế tổng thể được cho trong TCVN 7383-1:2004, điều 5). Một phần của quá trình này là sự đánh giá rủi ro mà các nguyên tắc của nó được cho trong TCVN 7301:2003. Sự đánh giá rủi ro bao hàm toàn bộ chu kỳ tuổi thọ của máy. Nếu tìm thấy có các rủi ro cần phải được giảm đi thì phải chọn các biện pháp thích hợp. TCVN 7383-2:2004 hướng dẫn các biện pháp để giảm rủi ro.

Một phần của quá trình giảm rủi ro là để xác định các chức năng an toàn (TCVN 7384-1:2004, 3.6) của máy. Phần này bao gồm các chức năng an toàn của hệ thống điều khiển, ví dụ, chức năng dừng khẩn cấp, khởi động và khởi động lại [xem TCVN 7384-1:2004, điều 5].

Một chức năng an toàn có thể được thực hiện bởi một hoặc nhiều bộ phận an toàn liên quan của hệ thống điều khiển. Người thiết kế có thể sử dụng các công nghệ nào đó, đơn hoặc tổ hợp. Một chức năng

an toàn cũng có thể là một chức năng vận hành, ví dụ, điều khiển bằng hai tay là biện pháp bắt đầu chu trình hoặc quá trình.

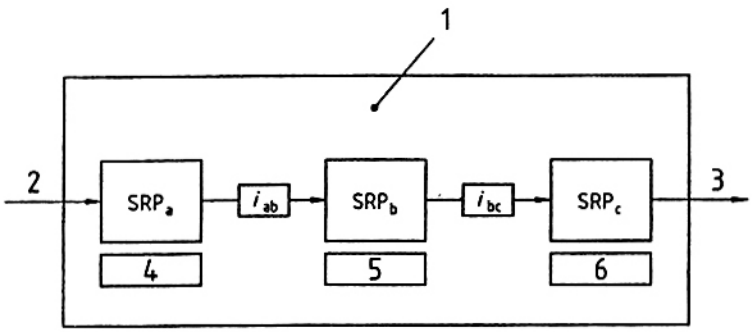
Trên hình 1 là một chức năng an toàn điển hình, nó chỉ ra các bộ phận an toàn liên quan (SRP) đối với:

- tín hiệu vào (SRP_a);
- tín hiệu logic / xử lý (SRP_b);
- tín hiệu ra / các phần tử điều khiển công suất (SRP_c);
- phương tiện nối mạng (i_{ab}, i_{bc}), ví dụ, điện, quang.

CHÚ THÍCH 1: Các bộ phận an toàn liên quan gồm một hoặc nhiều phần cấu thành; các phần cấu thành gồm có một hoặc nhiều phần tử.

CHÚ THÍCH 2: Tất cả các phương tiện nối mạng bao gồm trong các bộ phận an toàn liên quan.

CHÚ THÍCH 3: Ví dụ về một chức năng an toàn được giới thiệu trên hình 2 và các nội dung gắn liền với hình 2.



Chỉ dẫn

1 Chức năng an toàn điển hình
2 Biện pháp bắt đầu, ví dụ tác động tay, các tín hiệu khác
3 Hệ dẫn động máy, phương tiện ngắt, phanh
4 Tín hiệu vào
5 Tín hiệu logic
6 Tín hiệu ra

Hình 1 - Sơ đồ giới thiệu tổ hợp các bộ phận an toàn liên quan để xử lý một chức năng an toàn điển hình

Mỗi bộ phận an toàn liên quan của chức năng an toàn có thể được chế tạo từ các công nghệ khác nhau. Có thể dùng các công nghệ khác nhau trong bộ phận an toàn liên quan, ví dụ, một tín hiệu vào bao gồm một cơ cấu dẫn động cơ khí được nối với bộ biến đổi tín hiệu ánh sáng khởi động.

Khi thiết lập các chức năng an toàn của hệ thống điều khiển cần phải nhận ra các bộ phận an toàn liên quan của hệ thống điều khiển [xem TCVN7384-1:2004, 3.1 và điều 8] và quyết định xem sự đóng góp của chúng vào quá trình giảm rủi ro có tầm quan trọng đến mức nào. Các biện pháp bảo vệ do hệ thống điều khiển cung cấp phụ thuộc vào sự đóng góp này và không phụ thuộc trực tiếp vào việc giảm toàn bộ rủi ro đối với rủi ro đang xem xét.

CHÚ THÍCH 4: Sự mất đi chức năng an toàn không tự động dẫn đến thương tích hoặc tổn hại đến sức khoẻ nếu đã có các biện pháp bảo vệ hữu hiệu khác.

Sự giảm rủi ro tuỳ thuộc vào các bộ phận an toàn liên quan của hệ thống điều khiển càng lớn thì khả năng chống lại sai sót của các bộ phận này càng cao. [theo TCVN 7384-1:2004]. Do đó, về mặt nguyên tắc, cần phải có các biện pháp bảo vệ để giảm rủi ro.

- **Giảm xác suất xảy ra các sai sót ở phần cấu thành.** Mục đích là giảm xác suất xẩy ra sai sót hoặc các dạng hư hỏng ảnh hưởng đến chức năng an toàn. Vấn đề này có thể được thực hiện bằng cách tăng độ tin cậy của các phần cấu thành, ví dụ, bằng cách lựa chọn các phần cấu thành đã qua thử thách và / hoặc áp dụng các nguyên tắc an toàn đã qua thử thách để ngăn chặn các sai sót hoặc các dạng hư hỏng nghiêm trọng. TCVN 7384-1:2004 không đưa ra quan niệm có tính hệ thống về các yêu cầu độ tin cậy.

- **Cải tiến kết cấu của hệ thống.** Mục đích là tránh ảnh hưởng nguy hiểm của sai sót. Một số sai sót có thể được phát hiện và có thể cần đến kết cấu dư thừa và / hoặc kết cấu được giám sát.

Có thể dùng cả hai biện pháp riêng biệt nhau hoặc kết hợp với nhau. Với một số công nghệ, việc giảm rủi ro yêu cầu có thể đạt được bằng việc chọn các phần cấu thành tin cậy được và các biện pháp ngăn chặn sai sót, nhưng với các công nghệ khác thì việc giảm rủi ro có thể cần đến hệ thống dư thừa và / hoặc hệ thống được giám sát có hai hoặc nhiều bộ phận. Ngoài ra, cần tính đến các hư hỏng chung. Phương pháp mô tả các biện pháp này là sử dụng 5 loại được xác lập trong TCVN 7384-1:2004, điều 6.

4 Loại

Loại [xem định nghĩa trong TCVN 7384-1:2004, 3.2] được dùng để phân loại các bộ phận an toàn liên quan của hệ thống điều khiển, các bộ phận này thực hiện một chức năng an toàn dựa trên cơ sở tính năng của chúng trong trường hợp có sai sót. Các bộ phận này có thể được dùng đơn lẻ hoặc tổ hợp. Các loại cần được xem là các điểm tham khảo để làm một bộ phận an toàn liên quan của hệ thống điều khiển về mặt xảy ra các sai sót [xem TCVN 7384-1:2004]. Các loại không thể và không bao giờ được xem là có các giới hạn một cách chính xác, bởi vì sự đánh giá các thông số đang xem xét có thể là chủ quan.

Quan niệm chung là các loại của TCVN 7384-1:2004 luôn luôn hoặc cá biệt tương ứng với các mức rủi ro là không đúng

Trong khi lựa chọn một loại, người thiết kế cần xem xét đến tính năng an toàn đạt được và điều này phụ thuộc vào cả kết cấu và độ tin cậy của các bộ phận an toàn liên quan này. TCVN 7384-1:2004 không qui định đầy đủ các yêu cầu độ tin cậy.

Vì vậy tất cả các vấn đề có thể nói về tính năng an toàn đối với một công nghệ đã cho là:

a) các loại 1, 2, 3 và 4 đều tốt hơn loại B;

b) trong các loại B, 1 và 2, một sai sót đơn cũng có thể làm mất đi chức năng an toàn;

c) các loại 3 và 4 sẽ không bị hư hỏng do một sai sót đơn (các sai sót chung được xem như một sai sót đơn);

d) loại 4 có tính năng tốt nhất về mặt chấp nhận sai sót bởi vì sự tích luỹ các sai sót sẽ được xem xét.

Các hệ thống điều khiển sử dụng một số công nghệ không thể luôn luôn thoả mãn được mỗi loại, ví dụ, mối liên kết cơ khí đáp ứng được yêu cầu của loại 1 nhưng lại không thể đáp ứng yêu cầu của các loại 3 hoặc 4. Tuy nhiên triển vọng sẽ thực hiện được chức năng an toàn của loại 1 có thể bằng hoặc lớn hơn so với một số hệ thống khác đáp ứng được các loại 2, 3 hoặc 4.

Khi một chức năng an toàn được thực hiện bởi nhiều bộ phận an toàn liên quan của hệ thống điều khiển, có thể xảy ra ba khả năng:

a) mỗi một trong các bộ phận an toàn liên quan có cùng một loại và có thể được chỉ định cùng một loại chung cho toàn bộ các bộ phận an toàn liên quan;
b) các bộ phận an toàn liên quan được chỉ định các loại khác nhau nhưng được dùng tổ hợp với nhau theo cách sao cho có thể chỉ định được một loại chung;
c) không thể chỉ định được một loại chung bởi vì các công nghệ sử dụng không được thiết kế để đáp ứng cho mỗi loại.

Sự phát hiện một sai sót bởi hệ thống điều khiển trong loại 3 thường không cần thiết khi sai sót là hiển nhiên, ví dụ, khi máy tự bộc lộ sai sót bằng cách không cho phép khởi động hoặc khởi động lại.

Người xây dựng tiêu chuẩn loại C và người thiết kế cần quan tâm đến các giới hạn của việc đặt ra tính năng của chức năng an toàn dưới dạng một loại chung bởi vì các giới hạn trong các yêu cầu của loại, đặc biệt là đối với độ tin cậy.

5 Chọn loại

Khi chọn loại cho các bộ phận an toàn liên quan để thực hiện chức năng an toàn [xem TCVN 7384-1 : 2004, điều 6], cần xem xét các sai sót có thể xẩy ra theo hai khía cạnh:

- đánh giá xác suất hư hỏng hoặc ảnh hưởng của sai sót trong các bộ phận này;
- xem xét ảnh hưởng của hư hỏng hoặc sai sót trong các bộ phận này về chức năng an toàn.

Tính năng yêu cầu của chức năng an toàn phụ thuộc vào mức rủi ro; nếu mức rủi ro cao thì tính năng yêu cầu cần phải cao và ngược lại. Các tiêu chuẩn hài hoà thích hợp phản ánh tình trạng sáng tạo trong các ứng dụng khác nhau, và thông tin này cần được quan tâm khi chọn loại.

Xác suất xảy ra sai sót thường được xác lập bằng đánh giá định tính, bởi vì ít khi có đủ dữ liệu làm cơ sở cho đánh giá định lượng. Điều này có nghĩa là trong hầu hết các trường hợp cần dùng các dạng hư hỏng và phân tích ảnh hưởng (FMEA - xem IEC 60812) hoặc các phương pháp tương tự. Cần quan tâm đến tất cả các sai sót và / hoặc các dạng hư hỏng và tính năng thực tế của chức năng an toàn trong trường hợp có sai sót cần được kiểm tra so với tính năng yêu cầu.

Một số sai sót hoặc dạng hư hỏng có thể được ngăn chặn nếu xác suất xảy ra sai sót hoặc hư hỏng rất nhỏ. Xác suất này phụ thuộc vào các điều kiện ứng dụng. Điều quan trọng là tần số của các yêu cầu về chức năng an toàn có thể thay đổi lớn (từ các yêu cầu không thường xuyên, ví dụ, cơ cấu dừng khẩn

cấp, đến các yêu cầu liên tục, ví dụ, điều khiển các bộ phận chuyển động của máy). Vì lẽ đó, thường không thể đưa ra được các giá trị trung bình hoặc các đánh giá mức hư hỏng chấp nhận được.

Sau toàn bộ quá trình giảm rủi ro, việc công nhận cần được thực hiện [xem TCVN 7384-1:2004, điều 8]. Việc công nhận này là một phần của việc công nhận toàn bộ hệ thống máy.

Hình 2 là sơ đồ của các bộ phận an toàn liên quan cung cấp một trong những chức năng để điều khiển cơ cấu dẫn động máy. **Đây không phải là một sơ đồ chức năng /làm việc và được đưa ra chỉ để chứng minh nguyên tắc kết hợp các loại và các công nghệ trong một chức năng này.**

Việc điều khiển được thực hiện thông qua một mạch lôgic điều khiển điện tử và một van thủy lực hướng dòng, được kiểm tra tại các khoảng thời gian thích hợp [xem TCVN 7384-1:2004, 6.2.3]. Rủi ro được giảm đi bởi một bộ phận bảo vệ khoá liên động, ngăn ngừa sự tiếp cận tới tình trạng nguy hiểm khi bộ phận bảo vệ được đóng kín và ngăn chặn sự khởi động của cơ cấu dẫn động thuỷ lực khi bộ phận bảo vệ được mở.

Đối với ví dụ này, các bộ phận an toàn liên quan được tổ hợp lại của hệ thống điều khiển bắt đầu tại điểm 7 và kết thúc tại điểm 1 (xem hình 2).

Các bộ phận an toàn liên quan cung cấp chức năng an toàn là: cam bảo vệ, cơ cấu định vị, mạch logic điều khiển điện tử, van thủy lực hướng dòng và các phương tiện nối mạng.

Các bộ phận an toàn liên quan được tổ hợp này cung cấp một chức năng dừng (xem TCVN 7384-1:2004, 5.2) như là một chức năng an toàn (xem định nghĩa trong TCVN 7384-1:2004, 3.6). Khi bộ phận bảo vệ mở, các công tắc trong cơ cấu định vị mở và mạch logic điều khiển điện tử cung cấp một tín hiệu cho van thuỷ lực hướng dòng để dừng dòng thủy lực như là tín hiệu ra của các bộ phận an toàn liên quan của hệ thống điều khiển. Ở máy, tín hiệu này dừng chuyển động nguy hiểm của cơ cấu dẫn động.

Sự tổ hợp các bộ phận an toàn liên quan này tạo ra chức năng an toàn để chứng minh cho sự xếp loại dựa trên các yêu cầu của TCVN 7384-1:2004, điều 6. Nó xem xét khả năng và xác suất xảy ra sai sót có thể ảnh hưởng đến khả năng thực hiện chức năng an toàn của các bộ phận tổ hợp này. Khi dùng các nguyên tắc này, các bộ phận an toàn liên quan được chỉ ra trên hình 2 có thể được xếp loại như sau:

- Loại 1 đối với cơ cấu định vị cơ-điện tử

  Để giảm xác suất xảy ra sai sót, cơ cấu này bao gồm các phần cấu thành đã qua thử thách và áp dụng các nguyên tắc an toàn đã qua thử thách, ví dụ, thao tác mở dương, định kích thước quá mức (xem TCVN 7384-1:2004, điều 3 và 6.2.2);

- Loại 3 đối với mạch logic điều khiển điện tử

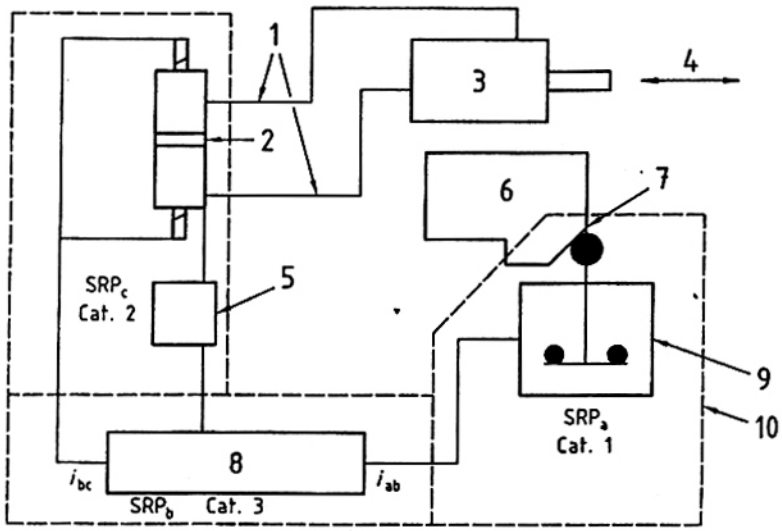
  Để tăng mức tính năng an toàn của mạch logic điều khiển điện tử này thì kết cấu của bộ phận an toàn liên quan của hệ thống điều khiển được thiết kế sao cho có thể phát hiện được hầu hết các sai sót đơn, ví dụ, sự dư thừa (xem TCVN 7384-1:2004, 6.2.4);

- Loại 2 đối với van thuỷ lực hướng dòng kiểm tra

  Để đạt được mức tính năng an toàn yêu cầu, bộ phận an toàn liên quan này sử dụng các phần cấu thành được kiểm tra định kỳ, ví dụ như giám sát, để phát hiện các sai sót không tránh được khi sử dụng các nguyên tắc an toàn đã qua thử thách (xem TCVN 7384-1:2004, 6.2.3).

Cũng cần phải tính đến vị trí, kích thước và sự lắp đặt các phương tiện nối mạng.

Mục tiêu chung là mỗi bộ phận an toàn liên quan đạt được mức tính năng an toàn tương tự sao cho sự đóng góp của các bộ phân an toàn liên quan của hệ thống điều khiển đưa ra được sự giảm rủi ro yêu cầu. Vì vậy cần quan tâm đến cả độ tin cậy và kết cấu của các bộ phận an toàn liên quan.



Chỉ dẫn

1 Tín hiệu ra
2 Van thuỷ lực hướng dòng
3 Các cơ cấu dẫn động thuỷ lực
4 Chuyển động nguy hiểm
5 Chức năng kiểm tra
6 Bộ phận bảo vệ
7 Tín hiệu vào
8 Mạch logic điều khiển điện tử
9 Cơ cấu định vị
10 Phạm vi của TCVN 7384-1:2004

CHÚ THÍCH - Các chức năng dừng và khởi động được bỏ qua để giữ cho ví dụ được đơn giản.

Hình 2 - Ví dụ giải thích việc sử dụng các loại

6 Vai trò của phụ lục B trong TCVN 7384-1:2004

Khi đánh giá rủi ro, cần theo các trình tự cho trong TCVN 7301: 2004. Khuyến cáo cho trong phụ lục B của TCVN 7384-1:2004 chỉ để tham khảo.

Thư mục

[1] TCVN 7384-1:2004 (ISO 12100-1:2003) An toàn máy - Khái niệm cơ bản, nguyên tắc chung cho thiết kế - Phần 1: Thuật ngữ cơ bản, phương pháp luận.

[2] TCVN 7383-2:2004 (ISO 12100-2:2003) An toàn máy - Khái niệm cơ bản, nguyên tắc chung cho thiết kế - Phần 2: Nguyên tắc kỹ thuật

[3] TCVN 7384-1:2004 (ISO 13849-1:1999) An toàn máy - Bộ phận an toàn liên quan của các hệ thống điều khiển - Phần 1: Nguyên tắc chung cho thiết kế.

[4] TCVN 7301:2003 (ISO 14121:1999) An toàn máy - Nguyên lý đánh giá rủi ro

[5] IEC 60812:2001 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) (Kỹ thuật phân tích về độ tin cậy của hệ thống - Phương pháp dùng cho dạng hư hỏng và phân tích các ảnh hưởng).

Quan hệ giữa các tiêu chuẩn quốc tế được trích dẫn trong tiêu chuẩn này và các tiêu chuẩn Châu Âu tương ứng

Tiêu chuẩn quốc tế	Tiêu chuẩn Châu Âu		Nhận xét
ISO 12100-1:2003 (TCVN 7383-1:2004)	EN 292-1:1991[a]	An toàn máy - Khái niệm cơ bản, nguyên tắc chung cho thiết kế - Phần 1: Thuật ngữ cơ bản, phương pháp luận	
ISO 12100-2:2003 (TCVN 7383-2:2004)	EN 292-2:1991/A1: 1995[a]	An toàn máy - Khái niệm cơ bản, nguyên tắc chung cho thiết kế - Phần 2: Nguyên tắc kỹ thuật	A1 của tiêu chuẩn EN không được xem xét trong ISO/TR
ISO 13849-1:1999 (TCVN 7384-1:2004)	EN 954-1:1996[a]	An toàn máy - Bộ phận an toàn liên quan của hệ thống điều khiển - Phần 1: Nguyên tắc chung cho thiết kế	
ISO 14121:1999 (TCVN 7301:2003)	EN 1050:1996[a]	An toàn máy - Nguyên lý đánh giá rủi ro.	
a) Tiêu chuẩn hài hoà theo chỉ dẫn về máy của Liên minh Châu Âu.			