TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 7384-1:2010
ISO 13849-1:2006

Xuất bản lần 2

AN TOÀN MÁY - CÁC BỘ PHẬN LIÊN QUAN ĐẾN AN TOÀN CỦA HỆ THỐNG ĐIỀU KHIỂN
PHẦN 1: NGUYÊN TẮC CHUNG VỀ THIẾT KẾ

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

HÀ NỘI – 2010

Mục lục

Lời nói đầu

TCVN 7384-1:2010 thay thế TCVN 7384-1:2004.

TCVN 7384-1:2010 hoàn toàn tương đương với ISO 13849-1:2006 và đính chính kỹ thuật 1:2009.

TCVN 7384-1:2010 do Ban kỹ thuật tiêu chuẩn quốc gia TCVN/TC 199 *An toàn máy* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ TCVN 7384 (ISO 13849), An toàn máy - Các bộ phận liên quan đến an toàn của hệ thống điều khiển gồm các phần sau:

- TCVN 7384-1:2010 (ISO 13849-1:2004), Phần 1: Nguyên tắc chung về thiết kế.

- TCVN 7384-2:2010 (ISO 13849-2:2003), Phần 2: Sự phê duyệt.

- TCVN 7384-100:2004 (ISO/TR 13849-100:2000), Phần 100: Hướng dẫn sử dụng và áp dụng TCVN 7384-1 (ISO 13849-1).

Lời giới thiệu

Cấu trúc của tiêu chuẩn an toàn trong lĩnh vực máy như sau:

a) Các tiêu chuẩn loại A (tiêu chuẩn cơ bản) đưa ra các khái niệm cơ bản, các nguyên tắc về thiết kế và những vấn đề chung có thể áp dụng cho máy.

b) Các tiêu chuẩn loại B (tiêu chuẩn an toàn chung) đề cập đến một hoặc nhiều khía cạnh về an toàn hoặc một hay nhiều kiểu thiết bị an toàn có thể sử dụng cho một phạm vi rộng các máy móc:

– Các tiêu chuẩn loại B1 đề cập đến các khía cạnh an toàn riêng (ví dụ, các khoảng cách an toàn, nhiệt độ bề mặt, tiếng ồn);

– Các tiêu chuẩn loại B2 đề cập đến trang thiết bị an toàn (ví dụ, các cơ cấu điều khiển hai tay, các cơ cấu khoá liên động, các cơ cấu nhạy cảm áp suất, các thiết bị bảo vệ).

c) Các tiêu chuẩn loại C (tiêu chuẩn an toàn của máy) đề cập đến các yêu cầu chi tiết về an toàn cho các máy hoặc nhóm máy cụ thể.

Tiêu chuẩn này là một tiêu chuẩn loại B như đã được giới thiệu trong TCVN 7383-1 (ISO 12100-1).

Khi các điều của tiêu chuẩn loại C khác với các điều được giới thiệu trong các tiêu chuẩn loại A hoặc loại B thì các điều của tiêu chuẩn loại C được ưu tiên sử dụng so với các điều của các tiêu chuẩn khác đối với các máy đã được thiết kế và chế tạo theo các điều của tiêu chuẩn loại C.

Tiêu chuẩn này đưa ra hướng dẫn cho các tiêu chuẩn có liên quan đến thiết kế và đánh giá các hệ thống điều khiển và cho các ban kỹ thuật soạn thảo các tiêu chuẩn loại B2 hoặc C được xem là tuân theo các yêu cầu cơ bản về an toàn trong Phụ lục I của hướng dẫn 98/37/EC, hướng dẫn máy. Tiêu chuẩn này không đưa ra hướng dẫn riêng về sự phù hợp với các hướng dẫn khác của EC.

Với tư cách là một bộ phận của chiến lược giảm rủi ro chung cho một máy nào đó, nhà thiết kế thường lựa chọn một số biện pháp để giảm rủi ro thông qua việc áp dụng các thiết bị an toàn có một hoặc nhiều chức năng an toàn.

Các bộ phận của hệ thống điều khiển máy móc cung cấp các chức năng an toàn được gọi là các bộ phận liên quan đến an toàn của các hệ thống điều khiển (SRP/CS) và các bộ phận này có thể bao gồm phần cứng và phần mềm và có thể tách rời khỏi hệ thống điều khiển của máy hoặc là một bộ phận gắn liền với hệ thống điều khiển của máy. Ngoài ra, để cung cấp chức năng an toàn thì các bộ phận liên quan đến an toàn của các hệ thống điều khiển cũng có thể cung cấp các chức năng vận hành (ví dụ, các cơ cấu điều khiển bằng hai tay là phương tiện cho sự khởi đầu của quá trình).

Khả năng của các bộ phận liên quan đến an toàn của các hệ thống điều khiển (SRP/CS) để thực hiện chức năng an toàn trong các điều kiện cho trước được phân thành một trong năm mức gọi là các mức tính năng (PL).

Các mức tính năng này được định nghĩa dưới dạng xác suất của hư hỏng gây nguy hiểm trong một giờ (xem Bảng 3).

Xác suất của hư hỏng gây nguy hiểm của chức năng an toàn phụ thuộc vào nhiều yếu tố, bao gồm cả cấu trúc phần cứng và cấu trúc phần mềm, mức độ của cơ cấu phát hiện các lỗi hoặc khuyết tật [tầm tác dụng (vùng) của sự chẩn đoán (DC)], độ tin cậy của các thành phần [thời gian trung bình tới khi hư hỏng gây nguy hiểm ($MTTF_d$), hư hỏng do nguyên nhân chung (CCF)], quá trình thiết kế, ứng suất làm việc, điều kiện môi trường và qui trình vận hành.

Để trợ giúp cho nhà thiết kế và tạo điều kiện dễ dàng cho việc đánh giá mức tính năng (PL) đạt được, tài liệu này sử dụng một phương pháp dựa trên sự phân loại các cấu trúc theo chuẩn thiết kế riêng và trạng thái quy định trong các điều kiện có lỗi hoặc khuyết tật. Các loại này được phân phối vào một trong năm mức, được gọi là các loại B, 1, 2, 3 và 4.

Các mức tính năng và các loại có thể áp dụng cho các bộ phận liên quan đến an toàn của các hệ thống điều khiển, như:

– Thiết bị bảo vệ (ví dụ, các cơ cấu điều khiển bằng hai tay, các cơ cấu khoá liên động), các cơ cấu bảo vệ nhạy cảm với điện (ví dụ, cơ cấu bảo vệ quang điện), các cơ cấu bảo vệ nhạy cảm với áp suất;

– Các bộ điều khiển (ví dụ, bộ lôgic dùng cho các chức năng điều khiển, bộ xử lý dữ liệu, bộ giám sát, kiểm tra, v.v...), và

– Các phần tử điều khiển công suất (ví dụ, các rơle, van, v.v...), cũng như các hệ thống điều khiển thực hiện các chức năng an toàn ở tất cả các loại máy - từ các thiết bị đơn giản (ví dụ các máy móc nhỏ cho nhà bếp, hoặc các cửa và cửa ra vào tự động) đến các thiết bị chế tạo (ví dụ, các máy bao gói, máy in, máy dập, ép).

Tiêu chuẩn này cung cấp một cơ sở rõ ràng để có thể đánh giá được kết cấu và chất lượng làm việc của bất cứ ứng dụng nào của các bộ phận liên quan đến an toàn trong các hệ thống điều khiển (SRP/CS) (và máy), bởi phòng thử của bên thứ ba hoặc một phòng thử độc lập.

Thông tin về các ứng dụng nên dùng của IEC 62061 và TCVN 7384-1 (ISO 13849-1) quy định các yêu cầu cho thiết kế và thực hiện các hệ thống điều khiển liên quan đến an toàn của máy. Việc sử dụng các tiêu chuẩn trên phù hợp với phạm vi của chúng có thể đáp ứng các yêu cầu cơ bản về an toàn có liên quan. Bảng dưới đây tóm tắt phạm vi của IEC 62061 và tiêu chuẩn này.

Bảng 1 - Ứng dụng của IEC 62061 và TCVN 7384-1 (ISO 13849-1)

	Công nghệ thực hiện chức năng điều khiển liên quan đến an toàn	TCVN 7384-1 (ISO 13849-1)	IEC 62061
A	Không dùng điện, ví dụ thuỷ lực	X	Không bao hàm
B	Điện-cơ, ví dụ, rơle và/hoặc điện tử đơn giản	Hạn chế cho các cấu trúc lựa chọn[a] và đến PL = e	Tất cả các cấu trúc đến SIL3
C	Điện tử phức hợp, ví dụ điện tử lập trình	Hạn chế cho các cấu trúc lựa chọn[a] và đến PL = d	Tất cả các cấu trúc và đến SIL3
D	A được kết hợp với B	Hạn chế cho các cấu trúc lựa chọn[a] và đến PL = e	X[c]
E	C được kết hợp với B	Hạn chế cho các cấu trúc lựa chọn (xem Chú thích 1) và đến PL = d	Tất cả các cấu trúc và đến SIL3
F	C được kết hợp với A, hoặc C được kết hợp với A và B	X[b]	X[c]

X Chỉ ra rằng TCVN 7384-1 (ISO 13849-1) hoặc IEC 62061 lựa chọn công nghệ phù hợp với công nghệ đã nêu ở cột đầu.

[a] Các cấu trúc lựa chọn được xác định trong 6.2 để đưa ra cách tiếp cận đơn giản để định lượng các mức tính năng;

[b] Đối với điện tử phức hợp: sử dụng các cấu trúc lựa chọn theo tiêu chuẩn này đến PL = d hoặc bất cứ cấu trúc nào theo IEC 62061;

[c] Đối với công nghệ không dùng điện, sử dụng các bộ phận theo tiêu chuẩn này làm các hệ con.

An toàn máy - Các bộ phận liên quan đến an toàn của hệ thống điều khiển - Phần 1: Nguyên tắc chung về thiết kế

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu về an toàn và các nguyên tắc để thiết kế và tích hợp các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS), bao gồm cả thiết kế phần mềm. Đối với các SRP/CS. Tiêu chuẩn này quy định các đặc tính bao gồm cả mức tính năng yêu cầu để thực hiện các chức năng an toàn. Tiêu chuẩn này áp dụng cho SRP/CS mà không quan tâm đến loại công nghệ và năng lượng được sử dụng (điện, thuỷ điện, khí nén, cơ khí v.v...) đối với tất cả các loại máy.

Tiêu chuẩn này không quy định các chức năng an toàn hoặc các mức tính năng được dùng trong một trường hợp cụ thể.

Tiêu chuẩn này quy định các yêu cầu riêng cho các bộ phận liên quan đến an toàn của các hệ thống điều khiển (SRP/CS) khi sử dụng các hệ thống điện tử lập trình. Nó không quy định các yêu cầu riêng cho thiết kế các sản phẩm là các thành phần của SRP/CS. Tuy nhiên có thể sử dụng các nguyên tắc đã cho như là các cấp hoặc mức tính năng.

CHÚ THÍCH 1: Các ví dụ về sản phẩm là thành phần của SRP/CS, rơle, van có nam châm điện kiểu lõi dài, công tắc vị trí, bộ điều khiển logic lập trình (PLC), bộ điều khiển động cơ, cơ cấu điều khiển bằng hai tay, thiết bị nhạy cảm áp suất. Để thiết kế các sản phẩm này, phải tham khảo các tiêu chuẩn thích hợp, ví dụ, TCVN 7385 (ISO 13851), ISO 13856-1 và ISO 13856-2.

CHÚ THÍCH 2: Đối với định nghĩa của mức tính năng yêu cầu, xem 3.1.24.

CHÚ THÍCH 3: Các yêu cầu quy định trong tiêu chuẩn này cho hệ thống điện tử lập trình thích hợp với phương pháp thiết kế và triển khai các hệ thống điều khiển điện, điện tử và điện tử lập trình liên quan đến an toàn của máy được cho trong IEC 62061.

CHÚ THÍCH 4: Đối với phần mềm được nhúng liên quan đến an toàn cho các bộ phận PL_r = e, xem Điều 7, IEC 61508-3:1998.

CHÚ THÍCH 5: Xem thêm Bảng 1.

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 ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 7383-1:2004 (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.

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.

TCVN 7384-2:2010 (ISO 13849-2:2003), An toàn máy - Các bộ phận liên quan đến an toàn của hệ thống điều khiển - Phần 2: Sự phê duyệt.

TCVN 7301 (ISO 14121), An toàn máy - Nguyên lý đánh giá rủi ro.

ISO 60050-191:1990, *International electrotechnical vocabulary - Chapter 191: Dependability and quality of service, and IEC 60050-191-am1;1999 and IEC 60050-191-am 2:2002:1999, Amendment 1 and Amendment 2, International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service* (Thuật ngữ kỹ thuật điện quốc tế - Chương 191: Tính tin cậy và chất lượng phục vụ và IEC 60050-191-am 1:1999 và IEC 60050-191-am 2:2002:1999, bản sửa đổi 1 và bản sửa đổi 2, thuật ngữ kỹ thuật điện quốc tế. Chương 191 : Tính tin cậy và chất lượng phục vụ).

IEC 61508-3:1998, *Functional safety of electrical/electronic/progammable electronic safety-related systems - Part 3: Software requirements, and IEC 61508-3 Corr.1:1999, Corrigendum 1 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements* (An toàn chức năng của hệ thống điện/điện tử/điện tử lập trình liên quan đến an toàn - Phần 3: Yêu cầu của phần mềm, và IEC 61508-3 Corr.1:1999, Bản đính chính 1 - An toàn chức năng của hệ thống điện/điện tử/điện tử lập trình liên quan đến an toàn - Phần 3: Yêu cầu của phần mềm).

IEC 61508-4:1998, *Functional safety of electrical/electronic/progammable electronic safety-related systems - Part 4: Definitions and abbreviations, and IEC 61508-4 Corr.1:1999, Corrigendum 1 - Functional safety of electrical/electronic/progammable electronic safety-related systems - Part 4:*

Definitions and abbreviations (An toàn chức năng của hệ thống điện/điện tử/điện tử lập trình liên quan đến an toàn - Phần 4: Định nghĩa và chữ viết tắt, và IEC 61508-4 Corr 1: 1999, Bản đính chính 1 - An toàn chức năng của hệ thống điện/điện tử/điện tử lập trình liên quan đến an toàn - Phần 4: Định nghĩa và chữ viết tắt).

3 Thuật ngữ, định nghĩa, ký hiệu và thuật ngữ viết tắt

3.1 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa cho trong TCVN 7383-1 (ISO 12100-1), IEC 60050-191 và các thuật ngữ định nghĩa sau:

3.1.1

Bộ phận liên quan đến an toàn của hệ thống điều khiển (safety-related part of a control system) SRP/CS
Bộ phận của hệ thống điều khiển đáp ứng các tín hiệu nhập liên quan đến an toàn và tạo ra các tín hiệu xuất liên quan đến an toàn.

CHÚ THÍCH 1: Các bộ phận liên quan đến an toàn tổ hợp của một hệ thống điều khiển khởi động tại điểm mà ở đó các tín hiệu nhập liên quan đến an toàn bắt đầu (bao gồm, ví dụ cả cam dẫn động và con lăn của công tắc vị trí) và kết thúc tại đầu ra của các phần tử điều khiển công suất (bao gồm các công tắc chính của một công tắc tơ).

CHÚ THÍCH 2: Nếu sử dụng các hệ thống giám sát để chẩn đoán thì chúng cũng được xem là bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS).

3.1.2

Loại (category)
Sự phân loại các bộ phận liên quan đến an toàn của một hệ thống điều khiển (SRP/CS) về khả năng chống lại các lỗi và trạng thái tiếp sau của chúng trong điều kiện có lỗi và sự phân loại này đạt được bằng cách bố trí kết cấu của các bộ phận, sự phát hiện lỗi và/hoặc độ tin cậy của SRP/CS.

3.1.3

Lỗi (fault)
Trạng thái của một bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) được đặc trưng bằng việc không có khả năng thực hiện một chức năng yêu cầu, trừ việc không có khả năng trong quá trình bảo dưỡng dự phòng hoặc các hoạt động khác theo kế hoạch hoặc do thiếu các nguồn cung cấp bên ngoài.

CHÚ THÍCH 1: Một lỗi thường dẫn đến một hư hỏng của bản thân bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) nhưng có thể không xuất hiện trước khi hư hỏng.

[IEC 60050-191:1990-05-01].

CHÚ THÍCH 2: Trong tiêu chuẩn này, "lỗi" có nghĩa là lỗi ngẫu nhiên.

3.1.4

Hư hỏng (failure)

Sự mất hoàn toàn khả năng thực hiện chức năng yêu cầu của một bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS).

CHÚ THÍCH 1: Sau một hư hỏng, bộ phận liên quan đến an toàn của hệ thống điều khiển có một lỗi.

CHÚ THÍCH 2: "Hư hỏng" là một sự kiện, khác với "lỗi" là một trạng thái.

CHÚ THÍCH 3: Khái niệm đã được định nghĩa không áp dụng cho bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) chỉ gồm có phần mềm. [IEC 60050-191:1990, 04-01].

CHÚ THÍCH 4: Các hư hỏng chỉ ảnh hưởng đến khả năng có thể dùng được của quá trình được điều khiển không thuộc phạm vi của tiêu chuẩn này.

3.1.5

Hư hỏng nguy hiểm (dangerous failure)

Hư hỏng có khả năng làm bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) lâm vào tình trạng nguy hiểm hoặc không hoạt động được.

CHÚ THÍCH 1: Tiềm năng có thể trở thành hiện thực hoặc không trở thành hiện thực có thể phụ thuộc vào cấu trúc kênh của hệ thống; trong các hệ thống dư thừa, một hư hỏng nguy hiểm của phần cứng ít có khả năng dẫn đến tình trạng nguy hiểm giới hạn hoặc không hoạt động được.

CHÚ THÍCH 2: Được sửa đổi cho hợp với IEC 61508-4:1998, định nghĩa 3.6.7.

3.1.6

Hư hỏng do nguyên nhân chung (common cause failure -CCF)

Hư hỏng của các bộ phận liên quan đến an toàn khác nhau của hệ thống điều khiển (SRP/CS) chỉ do một sự kiện, ở đó các hư hỏng này không phải là hậu quả của nhau.

[IEC 60050-191-1am1:1999, 04-23].

CHÚ THÍCH: Không nên nhầm lẫn hư hỏng do nguyên nhân chung với hư hỏng dạng chung (xem TCVN 7383-1:2004 (ISO 12100-1:2003), 3.34).

3.1.7

Hư hỏng có hệ thống (systematic failure)

Hư hỏng có liên quan đến một nguyên nhân nhất định theo một cách xác định, chỉ có thể được loại trừ bằng cải tiến thiết kế hoặc quá trình chế tạo, quy trình vận hành, tài liệu kỹ thuật hoặc các yếu tố có liên quan khác.

CHÚ THÍCH 1: Sự bảo dưỡng hiệu chỉnh mà không có sự cải biến thường không loại bỏ được nguyên nhân gây hư hỏng.

CHÚ THÍCH 2: Có thể tạo ra hư hỏng có hệ thống bằng cách mô phỏng nguyên nhân gây hư hỏng.

[IEC 60050-191:1990, 04-19].

CHÚ THÍCH 3: Ví dụ về các nguyên nhân của hư hỏng có hệ thống bao gồm lỗi của con người trong.

- Bản liệt kê các yêu cầu về an toàn;
- Thiết kế, chế tạo, lắp đặt, vận hành phần cứng, và
- Thiết kế, thực hiện v.v. của phần mềm.

3.1.8

Sự tạm ngừng (muting)

Sự ngừng tự động tạm thời của một hoặc nhiều chức năng an toàn bằng bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS).

3.1.9

Chỉnh đặt lại bằng tay (manual reset)

Chức năng trong bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) dùng để khôi phục lại bằng tay một hoặc nhiều chức năng an toàn trước khi khởi động lại máy.

3.1.10

Tổn hại (harm)

Sự tổn thương của thân thể hoặc thiệt hại cho sức khoẻ.

[TCVN 7383-1:2004 (ISO 12100-1:2003), 3.5].

3.1.11

Mối nguy hiểm (hazard)

Nguồn tổn hại có tiềm năng.

CHÚ THÍCH 1: Một mối nguy hiểm có thể có đủ khả năng để xác định nguồn gốc của nó (ví dụ, mối nguy hiểm về cơ, mối nguy hiểm về điện) hoặc bản chất của tổn hại có tiềm năng (ví dụ, mối nguy hiểm chập điện, mối nguy hiểm cắt (đứt), mối nguy hiểm do chất độc, mối nguy hiểm cháy).

CHÚ THÍCH 2: Mối nguy hiểm được nêu trong định nghĩa này:

- Hoặc có mặt thường xuyên trong quá trình sử dụng máy theo hướng dẫn (ví dụ, chuyển động của các bộ phận di động nguy hiểm, hồ quang điện trong quá trình hàn, tư thế có hại đến sức khoẻ, sự phát ra tiếng ồn, nhiệt độ cao);
- Hoặc xuất hiện bất ngờ (ví dụ, nổ, mối nguy hiểm bị nghiền, đập do hậu quả của sự khởi động không có chủ định/bất ngờ, mối nguy hiểm phun trào do hậu quả của sự gẫy vỡ, mối nguy hiểm rơi, đổ do hậu quả của sự tăng tốc/giảm tốc).

[TCVN 7383-1:2004 (ISO 12100-1:2003), 3.6].

3.1.12

Tình trạng nguy hiểm (hazardous situation)

Hoàn cảnh trong đó một người bị phơi ra trước ít nhất là một mối nguy hiểm, sự phơi này có khả năng dẫn đến tổn hại tức thời hoặc trong một khoảng thời gian dài.

[TCVN 7383-1:2004 (ISO 12100-1:2003), 3.9].

3.1.13

Rủi ro (risk)
Tổ hợp của xác suất xảy ra sự tổn hại và tính nghiêm trọng của tổn hại này.

[TCVN 7383-1:2004 (ISO 12100-1:2003) 3.11].

3.1.14

Rủi ro dư (residual risk)
Rủi ro còn lại sau khi đã có các biện pháp bảo vệ.

Xem Hình 2.

CHÚ THÍCH: Được sửa lại cho thích hợp từ TCVN 7383-1:2004 (ISO 12100-1:2003), định nghĩa 3.12.

3.1.15

Đánh giá rủi ro (risk assessment)
Quá trình tổng thể gồm có phân tích rủi ro và ước lượng rủi ro.

[TCVN 7383-1:2004 (ISO 12100-1:2003), 3.13].

3.1.16

Phân tích rủi ro (risk analysis)
Tổ hợp đặc điểm các giới hạn của máy, sự nhận dạng mối nguy hiểm và dự tính rủi ro.

[TCVN 7383-1:2004 (ISO 12100-1:2003), 3.14].

3.1.17

Ước lượng rủi ro (risk evaluation)
Sự xét đoán, dựa trên cơ sở phân tích rủi ro, xem các mục tiêu giảm rủi ro có đạt được hay không.

[TCVN 7383-1:2004 (ISO 12100-1:2003), 3.16].

3.1.18

Sử dụng máy theo hướng dẫn (intended use of machine)
Sử dụng máy theo thông tin quy định trong bản hướng dẫn sử dụng [TCVN 7383-1:2004 (ISO 12100-1:2003), 3.22].

3.1.19

Sử dụng sai hợp lý thấy trước (reasonably foreseeable misuse)
Sử dụng máy theo cách không được dự định của người thiết kế nhưng việc sử dụng này có thể do khả năng đoán trước được một cách dễ dàng của con người.

[TCVN 7383-1:2004 (ISO 12100-1:2003), 3.23].

3.1.20

Chức năng an toàn (safety function)

Chức năng của máy mà hư hỏng của nó có thể dẫn đến việc tăng lên tức thời các rủi ro.

[TCVN 7383-1:2004 (ISO 12100-1:2003), 3.28].

3.1.21

Giám sát (monitoring)

Chức năng an toàn bảo đảm một biện pháp bảo vệ được khởi động nếu khả năng của một bộ phận hoặc một thành phần để thực hiện chức năng của nó bị suy giảm hoặc nếu các điều kiện của quá trình công nghệ thay đổi theo hướng làm cho rủi ro tăng lên.

3.1.22

Hệ thống điện tử lập trình (programmable eletronic system) PES

Hệ thống điều khiển, bảo vệ hoặc giám sát dựa vào một hoặc nhiều thiết bị điện tử lập trình để hoạt động, bao gồm tất cả các thành phần của hệ thống như các nguồn cung cấp năng lượng, các cảm biến và các thiết bị nhập khác, các công tắc tơ và các thiết bị xuất khác.

CHÚ THÍCH: Đã được sửa đổi cho thích hợp từ IEC 61508-4:1998, định nghĩa 3.3.2.

3.1.23

Mức tính năng (performance level), PL

Mức riêng biệt dùng để quy định khả năng thực hiện một chức năng an toàn của các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) trong điều kiện đã cho.

CHÚ THÍCH: Xem 4.5.1.

3.1.24

Mức tính năng yêu cầu (required performance level), PL_r

Mức tính năng (PL) được áp dụng để đạt được sự giảm rủi ro yêu cầu đối với mỗi chức năng an toàn.

Xem các Hình 2 và A.1.

3.1.25

Thời gian trung bình đến khi hư hỏng nguy hiểm (mean time to dangerous failure), $MTTF_d$

Thời gian trung bình kỳ vọng đến khi xảy ra hư hỏng nguy hiểm.

CHÚ THÍCH: Được sửa đổi cho thích hợp từ IEC 62061:2005, định nghĩa 3.2.34.

3.1.26

Vùng chẩn đoán (diagnostic coverage), DC

Phạm vi chẩn đoán có hiệu quả có thể được xác định bằng tỷ số giữa mức hư hỏng của các hư hỏng nguy hiểm được phát hiện và mức hư hỏng của tổng các hư hỏng nguy hiểm.

CHÚ THÍCH 1: Vùng chẩn đoán có thể tồn tại đối với toàn thể hoặc các bộ phận của một hệ thống điều khiển. Ví dụ, vùng chẩn đoán có thể có đối với các cảm biến và/hoặc hệ thống logic và/hoặc các phần tử chấp hành.
CHÚ THÍCH 2: Được sửa đổi cho thích hợp từ IEC 61508-4:1998, định nghĩa 3.8.6.

3.1.27

Biện pháp bảo vệ (protective measure)

Biện pháp được dùng để đạt được sự giảm rủi ro.

VÍ DỤ 1: Do người thiết kế thực hiện: thiết kế bảo vệ, các biện pháp bảo vệ và bảo vệ bổ sung, thông tin cho sử dụng.

VÍ DỤ 2: Do người thiết kế thực hiện: tổ chức (quy trình làm việc an toàn, giám sát, các hệ thống cho phép làm việc), cung cấp và sử dụng các trang bị bảo vệ an toàn bổ sung, trang bị bảo vệ cá nhân, đào tạo.

CHÚ THÍCH: Được sửa đổi cho thích hợp từ TCVN 7383-1:2004 (ISO 12100-1:2003), định nghĩa 3.18.

3.1.28

Thời gian làm việc (mission time), T_M

Khoảng thời gian dành cho việc sử dụng theo hướng dẫn của một bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS).

3.1.29

Tần suất kiểm tra (test rate) r_t

Tần suất của các kiểm tra tự động để phát hiện các lỗi trong một bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS), là trị số nghịch đảo của khoảng thời gian kiểm tra chẩn đoán.

3.1.30

Tần suất yêu cầu (demand rate), r_d

Tần suất của các yêu cầu đối với một tác động liên quan đến an toàn của bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS).

3.1.31

Tần suất sửa chữa (repair rate), r_r

Trị số nghịch đảo của khoảng thời gian từ khi phát hiện ra một hư hỏng nguy hiểm bằng một phép kiểm tra trực tuyến hoặc do sự trục trặc rõ ràng của hệ thống tới khi khởi động lại sự hoạt động sau sửa chữa hoặc thay thế hệ thống/bộ phận.

CHÚ THÍCH: Thời gian sửa chữa không bao gồm khoảng thời gian cần thiết cho phát hiện hư hỏng.

3.1.32

Hệ thống điều khiển máy (machine control system)

Hệ thống đáp ứng các tín hiệu nhập từ các bộ phận của máy, người vận hành, thiết bị điều khiển bên ngoài hoặc bất cứ tổ hợp nào của các đối tượng nêu trên và tạo ra các tín hiệu xuất làm cho máy vận hành tốt theo quy định.

CHÚ THÍCH: Hệ thống điều khiển máy có thể sử dụng mọi công nghệ hoặc mọi tổ hợp các công nghệ khác nhau (ví dụ, điện/điện tử, thuỷ lực, khí nén, cơ khí).

3.1.33

Mức toàn vẹn của an toàn (safety integrity level), SIL

Mức riêng biệt (một trong số bốn mức) dùng để quy định yêu cầu về tính toàn vẹn của an toàn của các chức năng an toàn được cấp cho các hệ thống liên quan đến an toàn E/E/PE, trong đó cấp độ 4 là mức toàn vẹn của an toàn cao nhất và cấp độ 1 là mức toàn vẹn của an toàn thấp.

[IEC 61508-4:1998, 3.5.6].

3.1.34

Ngôn ngữ biến đổi giới hạn (limited variabity language), LVL

Loại ngôn ngữ có khả năng kết hợp các chức năng thư viện ứng dụng riêng được xác định trước để thực hiện việc đặc tả các yêu cầu an toàn.

CHÚ THÍCH 1: Được sửa đổi cho thích hợp từ IEC 61511-1:2003, định nghĩa 3.2.80.1.2.

CHÚ THÍCH 2: Các ví dụ điển hình của ngôn ngữ biến đổi có giới hạn (LVL) (Logic bậc thang, biểu đồ khối chức năng) được nêu trong IEC 61131-3.

CHÚ THÍCH 3: Một ví dụ điển hình của hệ thống sử dụng ngôn ngữ biến đổi có giới hạn (LVL); PLC (Bộ điều khiển logic lập trình).

3.1.35

Ngôn ngữ biến đổi hoàn toàn (full variability language), FVL

Loại ngôn ngữ có khả năng thực hiện rất nhiều chức năng và ứng dụng.

VÍ DỤ: C, C++, Bộ dịch hợp ngữ.

CHÚ THÍCH 1: Được sửa lại cho thích hợp từ IEC 61511-1:2003, định nghĩa 3.2.80.1.3.

CHÚ THÍCH 2: Một ví dụ điển hình của các hệ thống sử dụng ngôn ngữ biến đổi hoàn toàn (FVL): Hệ thống được nhúng.

CHÚ THÍCH 3: Trong lĩnh vực máy, ngôn ngữ biến đổi hoàn toàn (FVL) được dùng trong phần mềm được nhúng và ít được dùng trong phần mềm ứng dụng.

3.1.36

Phần mềm ứng dụng (application software)

Phần mềm dành riêng cho ứng dụng, do nhà sản xuất máy thực hiện, và thường chứa các dãy logic, các giới hạn và biểu thức điều khiển các dữ liệu nhập, xuất thích hợp, các tính toán và các quyết định cần thiết để đáp ứng các yêu cầu của bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS).

3.1.37

Phần mềm được nhúng, phần mềm hệ thống (embedded software, firmware, system software)

Phần mềm là một bộ phận của hệ thống do nhà sản xuất hệ thống điều khiển cung cấp và người sử dụng máy không thể truy cập để cải tiến được.

CHÚ THÍCH: Phần mềm được nhúng thường được viết bằng ngôn ngữ biến đổi hoàn toàn (FVL).

3.2 Ký hiệu và thuật ngữ viết tắt

Xem Bảng 2.

Bảng 2 – Ký hiệu và thuật ngữ viết tắt

Ký hiệu hoặc chữ viết tắt	Mô tả	Định nghĩa hoặc xuất hiện trong
a, b, c, d, e,	Ký hiệu các mức tính năng	Bảng 3
AOPD	Thiết bị bảo vệ quang điện tử phóng xạ (ví dụ, hàng rào ánh sáng)	Phụ lục H
B, 1, 2, 3, 4	Ký hiệu các loại	Bảng 7
B_{10d}	Số lượng chu kỳ tới khi 10 % các bộ phận hư hỏng một cách nguy hiểm (đối với các bộ phận khí nén và điện-cơ)	Phụ lục C
Cat.	Loại	3.1.2
CC	Bộ biến đổi dòng	Phụ lục I
CCF	Hư hỏng do nguyên nhân chung	3.1.6
DC	Vùng chẩn đoán	3.1.26
DC_{avg}	Vùng chẩn đoán trung bình	E.2
F, F1, F2	Tần suất và/hoặc thời gian phơi trước mối nguy hiểm	A.2.2
FB	Khối chức năng	4.6.3
FVL	Ngôn ngữ biến đổi hoàn toàn	3.1.35
FMEA	Dạng hư hỏng và phân tích ảnh hưởng	7.2
I, I1, I2	Thiết bị nhập, ví dụ, cảm biến	6.2
i, j	Chỉ số để đếm	Phụ lục D
I/0	Các khối nhập/xuất	Bảng E.1
i_{ab}, i_{bc}	Các phương tiện nối liên kết	Hình 4
K1A, K1B	Các công tắc tơ	Phụ lục I
L, L1, L2	Logic	6.2
LVL	Ngôn ngữ biến đổi giới hạn	3.1.34
M	Động cơ (mô tơ)	Phụ lục I
MTTF	Thời gian trung bình tới khi hư hỏng	Phụ lục C
$MTTF_d$	Thời gian trung bình tới khi hư hỏng nguy hiểm	3.1.25
n, N, $\overline{N}$	Số lượng các bộ phận	6.3, D1
N_{low}	Số lượng các SRP/CS có PL_{low} trong một tổ hợp của SRP/CS	6.3
O, O1, O2, OTE	Thiết bị xuất, ví dụ, thiết bị khởi động	6.2
P, P1, P2	Khả năng tránh nguy hiểm	A.2.3
PES	Hệ thống điện tử lập trình	3.1.22
PL	Mức tính năng	3.1.23
PLC	Bộ điều khiển logic lập trình	Phụ lục I

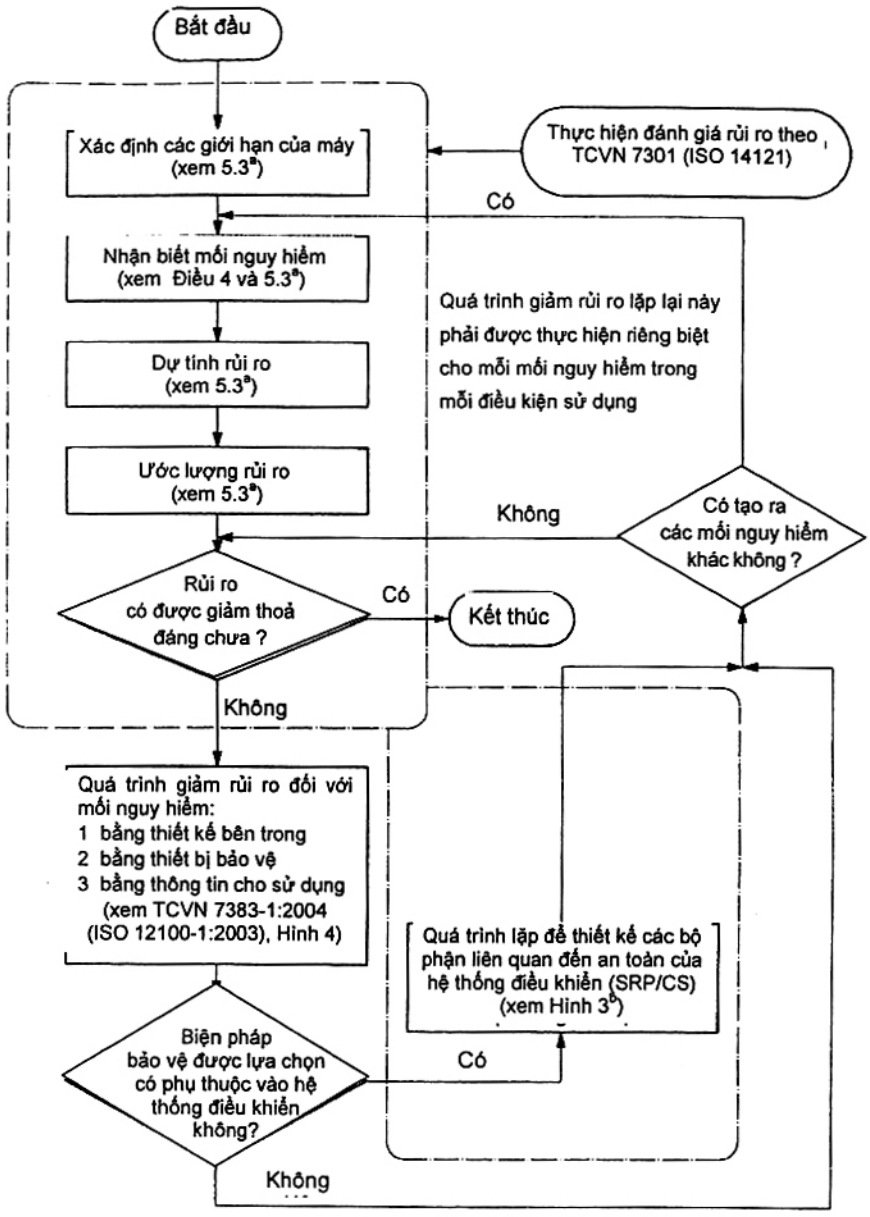
Bảng 2 (Kết thúc)

Ký hiệu hoặc chữ viết tắt	Mô tả	Định nghĩa hoặc xuất hiện trong
PL_{low}	Mức tính năng thấp nhất của SRP/CS trong tổ hợp của SRP/CS	6.3
PL_r	Mức tính năng yêu cầu	3.1.24
r_d	Tần suất của yêu cầu	3.1.30
RS	Cảm biến quay	Phụ lục I
S, S1, S2	Mức độ nghiêm trọng của thương tích	A.2.1
SW1A, SW1B, SW2	Công tắc tơ vị trí	Phụ lục I
SIL	Mức toàn vẹn của an toàn	Bảng 4
SRASW	Phần mềm ứng dụng liên quan đến an toàn	4.6.3
SRESW	Phần mềm được nhúng liên quan đến an toàn	4.6.2
SRP	Bộ phận liên quan đến an toàn	Chung
SRP/CS	Bộ phận liên quan đến an toàn của hệ thống điều khiển	3.1.1
TE	Thiết bị kiểm tra/thử nghiệm	6.2
T_M	Thời gian làm việc	3.1.28

4 Xem xét thiết kế

4.1 Mục tiêu an toàn trong thiết kế

Bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) phải được thiết kế và cấu tạo có tính đến các nguyên tắc của TCVN 7383-1 (ISO 12100-1) và TCVN 7301 (ISO 14121) một cách đầy đủ (xem Hình 1 và Hình 3). Phải xem xét toàn bộ việc sử dụng theo hướng dẫn và sử dụng sai hợp lý thấy trước.



[a] Tham chiếu TCVN 7383-1:2004 (ISO 12100-1:2003).
[b] Tham chiếu tiêu chuẩn này.

Hình 1 – Mô tả tóm tắt việc đánh giá rủi ro/giảm rủi ro

4.2 Kế hoạch để giảm rủi ro

4.2.1 Quy định chung

Chiến lược để giảm rủi ro ở máy được nêu trong TCVN 7383-1:2004 (ISO 12100-1:2003), Điều 5 và hướng dẫn bổ sung được nêu trong TCVN 7383-2:2004 (ISO 12100-2:2003), các Điều 4 (các biện pháp thiết kế sẵn có) và Điều 5 (các biện pháp bảo vệ và bảo vệ bổ sung). Chiến lược này bao hàm toàn bộ vòng đời của máy.

Quá trình phân tích mối nguy hiểm và giảm rủi ro đối với một máy yêu cầu phải loại trừ hoặc giảm các mối nguy hiểm thông qua một hệ thống các biện pháp theo trình tự:

- Loại trừ mối nguy hiểm hoặc giảm rủi ro bằng thiết kế [xem TCVN 7383-2:2004 (ISO 12100-2:2003), Điều 4];
- Giảm rủi ro bằng các biện pháp bảo vệ và bảo vệ bổ sung [xem TCVN 7383-2:2004 (ISO 12100-2:2003), Điều 5];
- Giảm rủi ro bằng cung cấp thông tin cho sử dụng về rủi ro còn dư [xem TCVN 7383-2:2004 (ISO 12100-2:2003), Điều 6].

4.2.2 Đóng góp của hệ thống điều khiển vào việc giảm rủi ro

Mục đích theo sau quy trình thiết kế tổng thể đối với máy là đạt được các mục tiêu an toàn (xem 4.1). Việc thiết kế bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) để giảm rủi ro yêu cầu là một phần không thể tách rời của quy trình thiết kế máy tổng thể. Bộ phận liên quan đến an toàn của hệ thống điều khiển có chức năng an toàn ở một mức tính năng (PL) để đạt được giảm rủi ro yêu cầu. Khi cung cấp chức năng an toàn với tư cách là một bộ phận an toàn vốn có của thiết kế hoặc là một bộ điều khiển đối với thiết bị bảo vệ thì việc thiết kế bộ phận liên quan đến an toàn của hệ thống điều khiển là một phần của chiến lược để giảm rủi ro. Đây là một quá trình lặp lại và được minh hoạ trên Hình 1 và Hình 3.

Đối với mỗi chức năng an toàn, các đặc tính (xem Điều 5) và mức tính năng yêu cầu phải được quy định và lập thành tài liệu các yêu cầu an toàn.

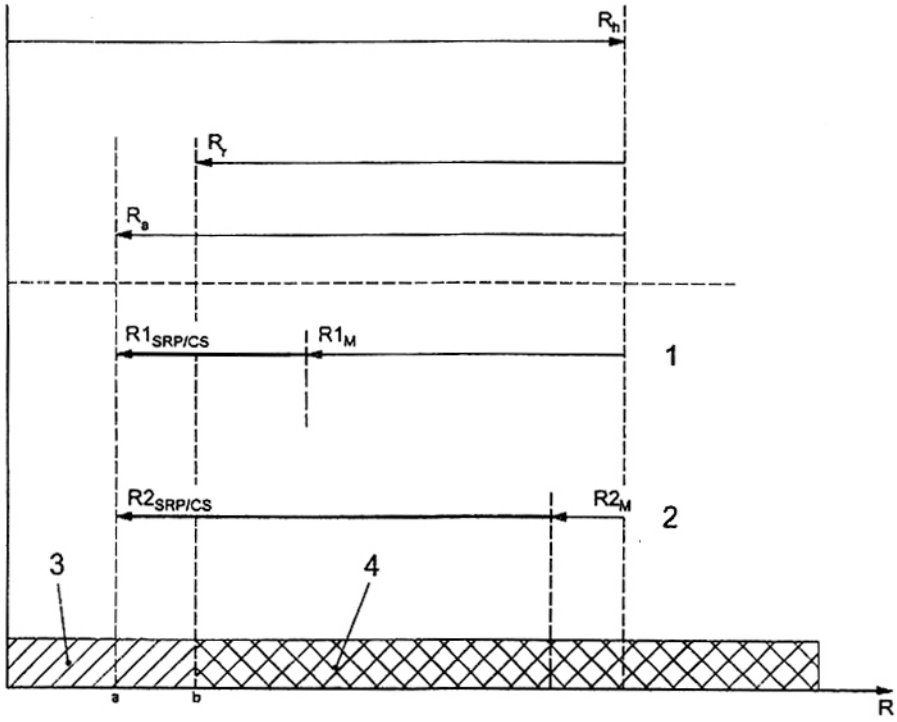
Trong tiêu chuẩn này các mức tính năng được xác định dưới dạng xác suất của hư hỏng nguy hiểm trên giờ. Có năm mức tính năng (a đến e) đã được xác lập với các phạm vi xác định của một hư hỏng nguy hiểm trên giờ (xem Bảng 3).

Bảng 3 - Mức tính năng (PL)

PL	Xác suất trung bình của hư hỏng nguy hiểm trên giờ, 1/h
a	$\geq 10^{-5}$ đến $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ đến $< 10^{-5}$
c	$\geq 10^{-6}$ đến $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ đến $< 10^{-6}$
e	$\geq 10^{-8}$ đến $< 10^{-7}$
CHÚ THÍCH: Ngoài xác suất trung bình của hư hỏng nguy hiểm trên giờ cũng cần có các biện pháp khác để đạt được PL.	

Từ việc đánh giá rủi ro [xem TCVN 7301 (ISO 14121)] ở máy, người thiết kế phải đóng góp vào quyết định giảm rủi ro mà mỗi chức năng an toàn có liên quan do bộ phận liên quan đến an toàn của hệ thống điều khiển thực hiện cần cung cấp. Sự đóng góp này không bao hàm toàn bộ rủi ro của máy được điều khiển, ví dụ, không phải là toàn bộ rủi ro của một máy ép cơ khí, hoặc một máy giặt được xem xét, nhưng phần rủi ro này được giảm đi do ứng dụng các chức năng an toàn riêng. Ví dụ về các chức năng an toàn này là chức năng dừng máy được bắt đầu bằng việc sử dụng một thiết bị bảo vệ nhạy cảm với điện trên máy ép hoặc chức năng khoá cửa của máy giặt.

Có thể đạt được việc giảm rủi ro bằng cách áp dụng nhiều biện pháp bảo vệ khác nhau (bao gồm cả việc sử dụng SRP/CS và không sử dụng SRP/CS) để có kết quả cuối là đạt được điều kiện an toàn (xem Hình 2).



CHÚ DẪN

R_h Đối với một tình trạng nguy hiểm riêng, rủi ro trước khi áp dụng các biện pháp bảo vệ.

R_r Giảm rủi ro được yêu cầu từ các biện pháp bảo vệ.

R_a Giảm rủi ro thực tế đạt được bằng các biện pháp bảo vệ.

1 Giải pháp 1: Phần quan trọng của giảm rủi ro do các biện pháp bảo vệ khác với SRP/CS (ví dụ, các biện pháp cơ khí), phần nhỏ của giảm rủi ro do SRP/CS.

2 Giải pháp 2: Phần quan trọng của giảm rủi ro do SRP/CS (ví dụ, màn ánh sáng), phần nhỏ của giảm rủi ro do các biện pháp bảo vệ khác với SRP/CS (ví dụ, các biện pháp cơ khí).

3 Rủi ro được giảm đi một các thoả đáng.

4 Rủi ro được giảm đi một cách không thoả đáng.

R Rủi ro.

a Rủi ro còn dư thu được bằng các giải pháp 1 và 2.

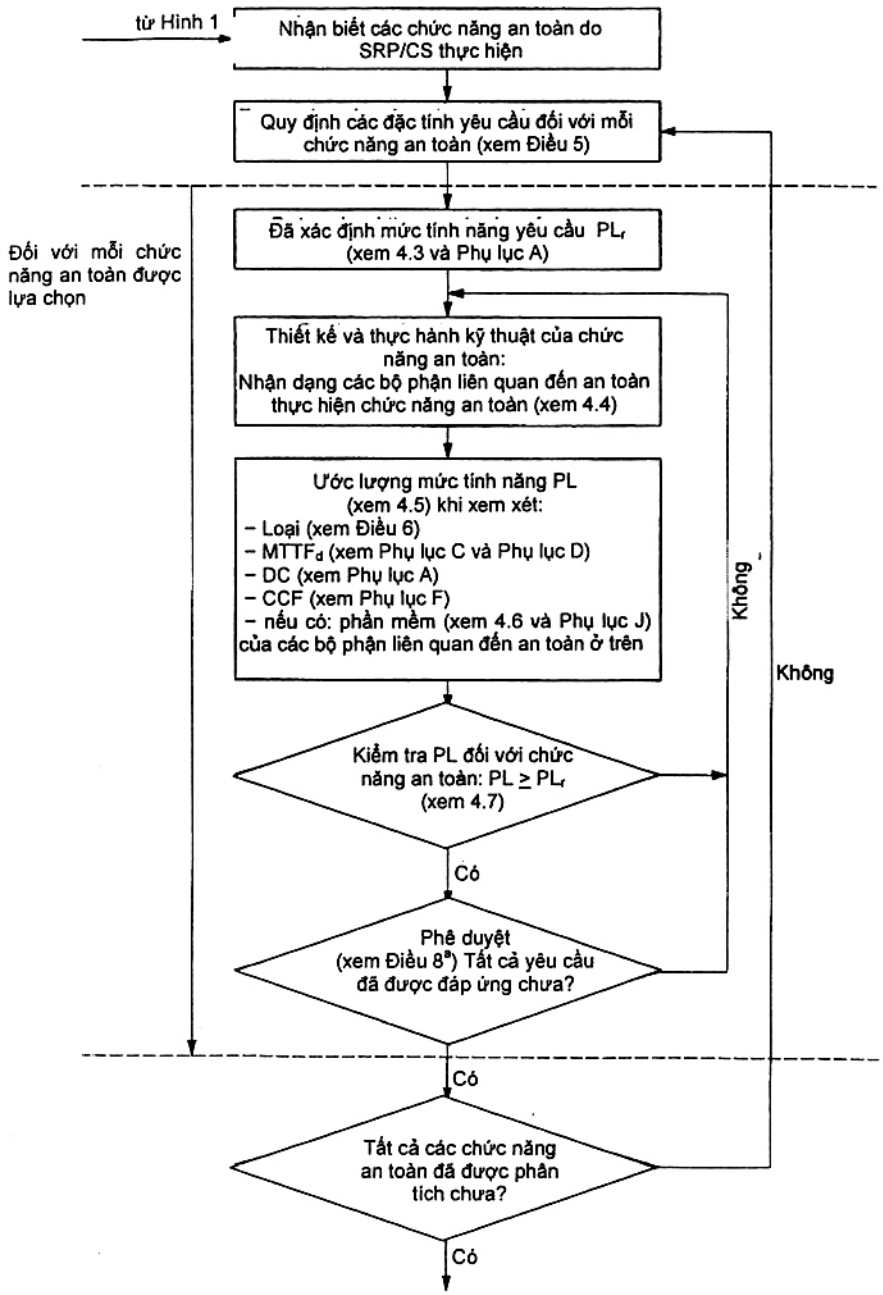
b Rủi ro được giảm đi một cách thỏa đáng.

$R1_{SRP/CS}$ $R2_{SRP/CS}$ giảm rủi ro từ chức năng an toàn được thực hiện bởi SRP/CS.

$R1_M$, $R2_M$ giảm rủi ro từ các biện pháp bảo vệ khác với SRP/CS (ví dụ, các biện pháp cơ khí)..

CHÚ THÍCH: Xem TCVN 7383 (ISO 12100) để có thêm thông tin về giảm rủi ro.

Hình 2 – Mô tả tóm tắt quá trình giảm rủi ro đối với mỗi tình trạng nguy hiểm



[a] TCVN 7384-2 (ISO 13849-2) đưa ra sự trợ giúp bổ sung cho sự phê duyệt.

Hình 3 – Quá trình lặp để thiết kế các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS)

4.3 Xác định mức tính năng yêu cầu (PL_r)

Đối với mỗi chức năng an toàn lựa chọn được thực hiện bởi SRP/CS phải xác định mức tính năng yêu cầu (PL_r) và lập thành tài liệu (xem Phụ lục A đối với hướng dẫn để xác định PL_r). Việc xác định mức tính năng yêu cầu là kết quả của đánh giá rủi ro và có liên quan đến lượng giảm rủi ro mà các bộ phận liên quan đến an toàn của hệ thống điều khiển phải thực hiện (xem Hình 2).

Lượng giảm rủi ro mà bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) cung cấp càng cao thì mức tính năng yêu cầu (PL_r) phải càng cao.

4.4 Thiết kế bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS)

Một phần của quá trình giảm rủi ro là xác định các chức năng an toàn của máy. Các chức năng an toàn của máy sẽ bao gồm các chức năng an toàn của hệ thống điều khiển, ví dụ, ngăn ngừa sự khởi động bất ngờ.

Một chức năng an toàn có thể được thực hiện bởi một hoặc nhiều bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) (ví dụ, bộ logic, phần tử điều khiển công suất). Một SRP/CS cũng có thể thực hiện các chức năng an toàn và các chức năng điều khiển tiêu chuẩn. Người thiết kế có thể sử dụng bất cứ công nghệ nào có thể sử dụng được, sử dụng từng công nghệ một hoặc kết hợp giữa các công nghệ. Bộ phận liên quan đến an toàn của hệ thống điều khiển cũng có thể cung cấp một chức năng vận hành (ví dụ, một AOPD là một phương tiện để bắt đầu chu trình).

Sự biểu thị bằng sơ đồ một chức năng an toàn điển hình trên Hình 4 chỉ ra một tổ hợp các bộ phận liên quan đến an toàn của các hệ thống điều khiển (SRP/CS) để.

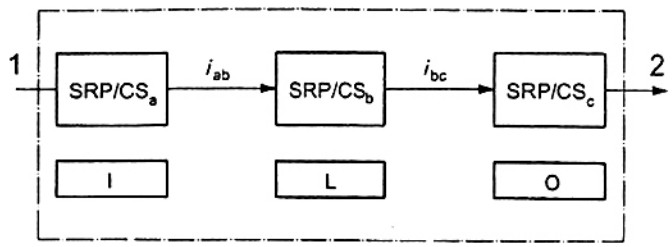
- Nhập (SRP/CS_a),
- Logic/xử lý (SRP/CS_b),
- Phần tử điều khiển xuất/công suất (SRP/CS_c), và
- Các biện pháp nối liên kết (i_{ab}, i_{bc}) (ví dụ, điện, quang).

CHÚ THÍCH 1: Trong cùng một máy, điều quan trọng là phải phân biệt giữa các chức năng an toàn khác nhau và các SRP/CS có liên quan của chúng khi thực hiện một chức năng an toàn nào đó.

Khi nhận dạng các chức năng an toàn của hệ thống điều khiển, người thiết kế phải nhận dạng SRP/CS (xem các Hình 1 và Hình 3) và, nếu cần thiết phải chỉ định chúng thực hiện chức năng nhập, logic và xuất và, trong trường hợp dư thừa phải chỉ định chúng thực hiện các kênh riêng và sau đó ước lượng mức PL (xem Hình 3).

CHÚ THÍCH 2: Các cấu trúc lựa chọn được cho trong Điều 6.

CHÚ THÍCH 3: Tất cả các phương tiện nối liên kết được bao gồm trong các bộ phận liên quan đến an toàn.



CHÚ DẪN

I Nhập

L Logic

0 Xuất

1 Sự kiện bắt đầu (ví dụ, khởi động bằng tay một nút ấn, mở bộ phận bảo vệ, dừng chùm tia của AOPD)

2 Cơ cấu dẫn động máy (ví dụ, phanh động cơ).

Hình 4 - Biểu thị bằng sơ đồ tổ hợp các bộ phận liên quan đến an toàn của các hệ thống điều khiển để xử lý chức năng an toàn điển hình

4.5 Ước lượng mức tính năng đạt được PL và mối quan hệ với SIL

4.5.1 Mức tính năng PL

Theo tiêu chuẩn này, khả năng của các bộ phận liên quan đến an toàn để thực hiện chức năng an toàn được biểu thị qua việc xác định mức tính năng.

Đối với mỗi SRP/CS và/hoặc tổ hợp của các SRP/CS được lựa chọn để thực hiện một chức năng an toàn thì phải dự tính mức tính năng PL.

Mức tính năng PL của SRP/CS phải được xác định bằng cách dự tính các thông số sau:

- Trị số $MTTF_d$ đối với các bộ phận đơn (xem Phụ lục C và Phụ lục D):
- DC (xem Phụ lục E);
- CCF (xem Phụ lục F);
- Cấu trúc (xem Điều 6);
- Trạng thái của chức năng an toàn trong điều kiện có lỗi (xem Điều 6);
- Phần mềm liên quan đến an toàn (xem 4.6 và Phụ lục J);
- Hư hỏng có hệ thống (xem Phụ lục G);
- Khả năng thực hiện một chức năng an toàn trong các điều kiện môi trường yêu cầu.

CHÚ THÍCH 1: Các thông số khác, ví dụ các thông số vận hành, tần suất của yêu cầu, tần suất kiểm tra cũng có thể ảnh hưởng.

Các thông số này có thể được hợp thành nhóm theo hai phương pháp có liên quan đến quá trình ước lượng:

a) Các thông số định lượng được (trị số $MTTF_d$ đối với các bộ phận đơn, DC, CCF, cấu trúc);

b) Các thông số định tính, không định lượng được có ảnh hưởng đến trạng thái của SRP/CS (trạng thái của chức năng an toàn trong các điều kiện có lỗi, phần mềm có liên quan đến an toàn, hư hỏng có hệ thống và các điều kiện môi trường).

Trong số các thông số định lượng được thì sự đóng góp của độ tin cậy (ví dụ, $MTTF_d$, cấu trúc) có thể thay đổi theo công nghệ được sử dụng. Ví dụ, có thể (trong các giới hạn nào đó) một kênh đơn của các bộ phận liên quan đến an toàn có độ tin cậy cao trong công nghệ để cho cùng một PL hoặc PL cao hơn so với một cấu trúc có lỗi có độ tin cậy thấp hơn trong một công nghệ khác.

Có nhiều phương pháp để dự tính các thông số định lượng được của PL cho bất cứ hệ thống nào (ví dụ, một hệ thống phức hợp), ví dụ, mô hình Markov, lưới Petri ngẫu nhiên tổng quát hoá (GSPN), sơ đồ khối độ tin cậy [ví dụ, xem IEC 61508].

Để đánh giá các thông số định lượng được của PL dễ dàng hơn, tiêu chuẩn này đưa ra một phương pháp đơn giản hoá dựa trên định nghĩa của năm cấu trúc được lựa chọn đáp ứng các tiêu chuẩn thiết kế riêng và trạng thái trong điều kiện có lỗi (xem 4.5.4).

Đối với một bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) hoặc tổ hợp của các bộ phận này được thiết kế theo các yêu cầu cho trong Điều 6 thì xác suất trung bình của một hư hỏng nguy hiểm có thể được dự tính bởi Hình 5 và quy trình cho trong các Phụ lục A đến Phụ lục H, Phụ lục J và Phụ lục K.

Đối với một bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) có sai lệch so với các cấu trúc được lựa chọn thì phải đưa ra tính toán chi tiết để chứng minh sự đạt được mức tính năng yêu cầu (PL_r).

Trong ứng dụng mà bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) có thể được xem là đơn giản và mức tính năng yêu cầu từ a đến c thì có thể đưa ra dự tính định tính về PL trong tính hợp lý của thiết kế.

CHÚ THÍCH 2: Để thiết kế các hệ thống điều khiển phức hợp, như hệ thống điện tử lập trình (PES) thì việc ứng dụng các tiêu chuẩn khác có thể là thích hợp (ví dụ, IEC 61508, IEC 62061 hoặc IEC 61496).

Việc đạt được các kết quả định tính của PL có thể được chứng minh bằng ứng dụng các biện pháp nên dùng được cho trong 4.6 và Phụ lục G.

Trong các tiêu chuẩn theo IEC 61508, khả năng thực hiện một chức năng an toàn của các hệ thống điều khiển liên quan đến an toàn được thể hiện thông qua mức toàn vẹn của an toàn (SIL). Bảng 4 chỉ ra mối quan hệ giữa hai khái niệm (PLs và SILs).

PL a không có sự tương ứng với thang SIL và được sử dụng chủ yếu để giảm rủi ro cua thương tích nhẹ, thường chữa khỏi được. Vì SIL 4 được dành cho các sự cố nghiêm trọng có thể xảy ra trong công nghiệp gia công nên phạm vi này không liên quan đến các rủi ro ở máy. PL e tương ứng với SIL 3 được xác định là mức cao nhất.

Bảng 4 – Quan hệ giữa mức tính năng (PL) và mức toàn vẹn của an toàn (SIL)

PL	SIL (tham khảo IEC 61508-1) chế độ vận hành cao/liên tục
a	Không tương ứng
b	1
c	1
d	2
e	3

Do đó phải áp dụng các biện pháp bảo vệ chính sau để giảm rủi ro:

- Giảm xác suất của các lỗi ở mức bộ phận. Mục đích là giảm xác suất của các lỗi hoặc hư hỏng ảnh hưởng đến chức năng an toàn. Điều này có thể thực hiện được bằng cách tăng độ tin cậy của các bộ phận, ví dụ bằng cách lựa chọn các bộ phận đã quen và đáng tin cậy và/hoặc áp dụng các nguyên tắc an toàn đã quen-đáng tin cậy, để giảm thiểu hoặc loại trừ các lỗi tới hạn hoặc hư hỏng [xem TCVN 7384-2 (ISO 13849-2)].
- Nâng cao kết cấu của bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/SC). Mục đích là để tránh ảnh hưởng nguy hiểm của lỗi. Một số lỗi có thể được phát hiện và có thể cần đến một cấu trúc dư thừa và/hoặc cấu trúc được giám sát.

Có thể áp dụng cả hai biện pháp riêng biệt hoặc kết hợp với nhau. Với một số công nghệ, việc giảm rủi ro có thể đạt được bằng cách lựa chọn các bộ phận đáng tin cậy và bằng cách loại trừ các lỗi; nhưng với các công nghệ khác, việc giảm rủi ro có thể phải cần đến một hệ thống dư thừa và/hoặc một hệ thống được giám sát. Ngoài ra, các hư hỏng do nguyên nhân chung (CCF) phải được tính đến (xem Hình 3).

Đối với các phản lực liên kết của cấu trúc, xem Điều 6.

4.5.2 Thời gian trung bình tới khi hư hỏng nguy hiểm của mỗi kênh ($MTTF_d$)

Giá trị của $MTTF_d$ của mỗi kênh được cho với ba mức (xem Bảng 5) và phải được tính đến cho mỗi kênh một cách riêng biệt (ví dụ, kênh đơn, mỗi kênh của một hệ thống dư thừa).

Theo $MTTF_d$, có thể tính đến giá trị lớn nhất là 100 năm.

Bảng 5 - Thời gian trung bình tới khi hư hỏng nguy hiểm của mỗi kênh ($MTTF_d$)

$MTTF_d$	
Ký hiệu của mỗi kênh	**Phạm vi của mỗi kênh**
Thấp	3 năm ≤ $MTTF_d$ < 10 năm
Trung bình	10 năm ≤ $MTTF_d$ < 30 năm
Cao	30 năm ≤ $MTTF_d$ ≤ 100 năm

CHÚ THÍCH 1: Việc lựa chọn các phạm vi $MTTF_d$ của mỗi kênh được dựa trên các tần suất hư hỏng tìm thấy ở mức phát triển kỹ thuật hiện tại, tạo thành một loại tỷ xích lôgarit phù hợp với tỷ xích lôgarit của PL. Một giá trị $MTTF_d$ của mỗi kênh nhỏ hơn ba năm không có hy vọng tìm thấy được đối với SRP/CS thực, bởi vì điều này có nghĩa là sau một năm sẽ có khoảng 30 % tất cả các hệ thống trên thị trường sẽ hư hỏng và cần được thay thế. Một giá trị $MTTF_d$ của mỗi kênh lớn hơn 100 năm là không chấp nhận được bởi vì SRP/CS đối với rủi ro cao không phụ thuộc vào độ tin cậy của riêng các bộ phận. Để gia cố SRP/CS chống lại hư hỏng có hệ thống và hư hỏng ngẫu nhiên, cần có các biện pháp bổ sung như hệ thống có liên kết dư thừa và tiến hành thử nghiệm. Để có tính khả thi, số lượng các phạm vi đã được hạn chế là ba. Giới hạn của các giá trị $MTTF_d$ của mỗi kênh tối đa là 100 năm được dùng cho kênh đơn của SRP/CS thực hiện chức năng an toàn. Có thể sử dụng các giá trị $MTTF_d$ cao hơn cho các bộ phận đơn (xem Bảng D.1).

CHÚ THÍCH 2: Các ranh giới của các phạm vi được chỉ ra trong bảng này có độ chính xác trong khoảng 5 %.

Để dự tính $MTTF_d$ của một bộ phận phải sử dụng quy trình tìm dữ liệu theo trình tự sau:

a) Dùng dữ liệu của nhà sản xuất;

b) Dùng các phương pháp trong các Phụ lục C và Phụ lục D;

c) Chọn 10 năm.

4.5.3 Vùng chẩn đoán (DC)

Giá trị của vùng chẩn đoán (DC) được cho theo bốn mức (xem Bảng 6). Để dự tính giá trị DC, trong hầu hết các trường hợp có thể sử dụng dạng hư hỏng và phân tích các ảnh hưởng (FMEA, xem IEC 60812) hoặc các phương pháp tương tự. Trong trường hợp này, nên xem xét tất cả các lỗi và/hoặc dạng hư hỏng có liên quan và kiểm tra mức tính năng (PL) của tổ hợp SRP/CS thực hiện chức năng an toàn so với mức tính năng yêu cầu (PL_r). Phương pháp đơn giản hoá để dự tính DC được giới thiệu trong Phụ lục E.

Bảng 6 – Vùng chẩn đoán (DC)

DC	
Ký hiệu	**Phạm vi của mỗi kênh**
Không	DC < 60 %
Thấp	60 % ≤ DC< 90 %
Trung bình	90 % ≤ DC< 99 %
Cao	99 % ≤ DC

CHÚ THÍCH 1: Đối với SRP/CS gồm nhiều bộ phận, sử dụng giá trị trung bình DC_{avg} trên Hình 5, Điều 6 và E2.

CHÚ THÍCH 2: Việc lựa chọn các phạm vi DC dựa trên các trị số chủ chốt 60 %, 90 % và 99 % đã được xác lập trong các tiêu chuẩn khác (ví dụ, IEC 61508) có liên quan đến vùng chẩn đoán của các phép thử nghiệm. Các kết quả nghiên cứu đã chỉ ra rằng (1-DC) là biện pháp đặc trưng hơn so với DC để đạt được hiệu quả của kiểm tra. (1-DC) đối với các trị số chủ chốt 60 %, 90 % và 99 % tạo thành một loại tỷ xích lôgarit phù hợp với tỷ xích lôgarit của PL. Một trị số DC nhỏ hơn 60 % chỉ có ảnh hưởng nhẹ đến độ tin cậy của hệ thống được thử nghiệm và do đó được gọi là "không". Một trị số DC lớn hơn 99 % đối với các hệ thống phức hợp rất khó có thể đạt được. Để có tính khả thi, số lượng các phạm vi đã được hạn chế là bốn. Các ranh giới của các phạm vi được chỉ ra trong bảng này có độ chính xác trong khoảng 5 %.

4.5.4 Quy trình đơn giản hoá để dự tính PL

Có thể dự tính mức tính năng (PL) bằng cách tính đến tất cả các thông số có liên quan và các phương pháp thích hợp để tính toán (xem 4.5.1). Điều này mô tả quy trình đơn giản hoá để dự tính PL của một SRP/CS dựa trên các cấu trúc đã lựa chọn. Một số cấu trúc khác có kết cấu tương tự có thể được biến đổi thành các cấu trúc đã lựa chọn này để thu được kết quả dự tính của PL.

Các cấu trúc đã lựa chọn được biểu thị dưới dạng các sơ đồ khối và được liệt kê trong ngữ cảnh của mỗi loại trong 6.2. Thông tin về phương pháp lập sơ đồ khối và các sơ đồ khối liên quan đến an toàn được nêu trong 6.2 và Phụ lục B.

Các cấu trúc đã lựa chọn thể hiện tính logic của kết cấu hệ thống đối với mỗi loại. Sự thực hiện về mặt kỹ thuật hoặc chẳng hạn như sơ đồ mạch chức năng có thể được xem là hoàn toàn khác nhau.

Các cấu trúc đã lựa chọn được vẽ cho tổ hợp SRP/CS, bắt đầu tại các điểm tại đó các tín hiệu liên quan đến an toàn được bắt đầu và kết thúc tại đầu ra của các phần tử điều khiển công suất [xem TCVN 7383-1:2004 (ISO 12100-1:2003), Phụ lục A]. Có thể sử dụng các cấu trúc đã lựa chọn để mô tả một bộ phận hoặc một bộ phận con của một hệ thống điều khiển, hệ thống này đáp ứng các tín hiệu nhập và tạo ra các tín hiệu xuất liên quan đến an toàn. Vì vậy phần tử "nhập" có thể biểu thị một màn

ánh sáng (AOPD) cũng như các mạch nhập của các phần tử điều khiển logic hoặc các công tắc nhập. "xuất" có thể biểu thị một tín hiệu xuất làm chuyển mạch thiết bị (OSSD) hoặc các tín hiệu xuất của các bộ quét laser.

Đối với các cấu trúc đã lựa chọn cần có các giả thiết điển hình sau:

- Thời gian làm việc 20 năm (xem Điều 10);
- Tần suất hư hỏng không đổi trong thời gian làm việc;
- Đối với loại 2, tần suất của yêu cầu ≤ 1/100 tần suất thử nghiệm;
- Đối với loại 2, $MTTFd_{,TE}$ lớn hơn một nửa $MTTF_{d,L}$.

CHÚ THÍCH: Khi các khối của mỗi kênh không thể tách ly được thì có thể áp dụng như sau: $MTTF_d$ của kênh thử nghiệm được tóm tắt (TE, OTE) lớn hơn một nửa $MTTF_d$ của kênh chức năng được tóm tắt (I, L,O).

Phương pháp học coi các loại như là các cấu trúc có vùng chẩn đoán trung bình (DC_{avg}) xác định. Mức tính năng (PL) của mỗi SRP/CS phụ thuộc vào cấu trúc, thời gian trung bình tới khi hư hỏng nguy hiểm ($MTTF_d$) trong mỗi kênh và DC_{avg}.

Nên tính đến các hư hỏng do nguyên nhân chung (CCF) (xem hướng dẫn trong Phụ lục F).

Đối với các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) có phần mềm cần áp dụng các yêu cầu trong 4.6.

Nếu không có các dữ liệu định lượng hoặc không dùng các dữ liệu định lượng (ví dụ, các hệ thống phức hợp thấp) thì nên lựa chọn trường hợp xấu nhất của tất cả các tham số có liên quan.

Một tổ hợp của SRP/CS hoặc một SRP/CS đơn có thể có một mức tính năng (PL). Tổ hợp của nhiều SRP/CS có PL khác nhau được xem xét trong 6.3.

Trong trường hợp các ứng dụng có mức tính năng yêu cầu (PL_r) từ a đến c thì phải có đủ các biện pháp để tránh các lỗi đối với các ứng dụng có rủi ro cao, PL_r từ d đến e, thì kết cấu của SRP/CS cần có các biện pháp để tránh, phát hiện hoặc chịu được lỗi. Các biện pháp thực tế bao gồm làm kết cấu dư thừa, đa dạng hoá kết cấu, kết cấu có kiểm soát [xem TCVN 7383-2:2004 (ISO 12100-2:2003), Điều 3 và IEC 60204-1:2000].

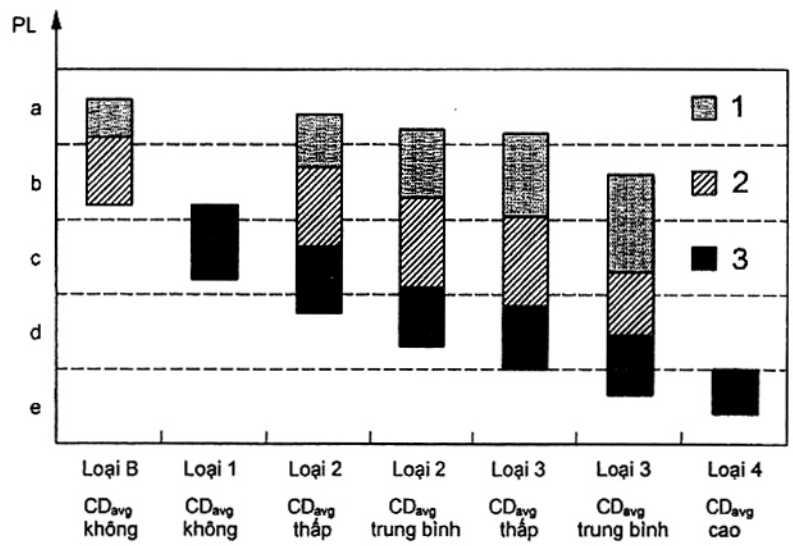
Hình 5 chỉ ra quy trình để lựa chọn các loại phối hợp với thời gian trung bình tới khi hư hỏng nguy hiểm ($MTTF_d$) và vùng chẩn đoán trung bình DC_{avg} để đạt được mức tính năng yêu cầu (PL_r) của chức năng an toàn

Để dự tính mức tính năng (PL), Hình 5 giới thiệu các sự phối hợp khác nhau có thể có của loại với DC_{avg} (trục nằm ngang) và $MTTF_d$ của mỗi kênh (các thanh). Các thanh trên biểu đồ biểu thị ba phạm vi $MTTF_d$ của mỗi kênh (thấp, trung bình và cao) có thể được lựa chọn để đạt được mức tính năng yêu cầu (PL_r).

Trước khi sử dụng phương pháp đơn giản hoá với Hình 5 (biểu thị các kết quả của các mô hình markov khác nhau dựa trên các cấu trúc đã lựa chọn của Điều 6) thì phải xác định loại SRP/CS cũng như DC_{avg} và $MTTF_d$ của mỗi loại kênh (xem Điều 6 và các Phụ lục C đến Phụ lục E).

Đối với các loại 2,3 và 4 phải thực hiện các biện pháp thoả đáng đối với hư hỏng do nguyên nhân chung (xem hướng dẫn trong Phụ lục F). Khi tính đến các thông số này, Hình 5 đưa ra phương pháp biểu đồ để xác định PL mà SRP/CS đã đạt được. Sự phối hợp loại (bao gồm hư hỏng do nguyên nhân chung) và DC_{avg} xác định cột nào của Hình 5 được lựa chọn. Theo $MTTF_d$ của mỗi kênh phải lựa chọn một trong ba diện tích được tô màu khác nhau của cột có liên quan.

Vị trí thẳng đứng của diện tích này xác định mức tính năng (PL) đạt được và mức tính năng này được đọc theo trục thẳng đứng. Nếu diện tích bao hàm hai hoặc ba mức tính năng thì mức tính năng đạt được được cho trong Bảng 7. Phụ lục K giới thiệu sự lựa chọn trị số chính xác hơn của PL phụ thuộc vào trị số chính xác của $MTTF_d$ của mỗi kênh.



CHÚ DẪN

PL Mức tính năng

1 $MTTF_d$ của mỗi kênh = thấp

2 $MTTF_d$ của mỗi kênh = trung bình

3 $MTTF_d$ của mỗi kênh = cao

Hình 5 – Quan hệ giữa các loại, DC_{avg}, $MTTF_d$ của mỗi kênh và PL

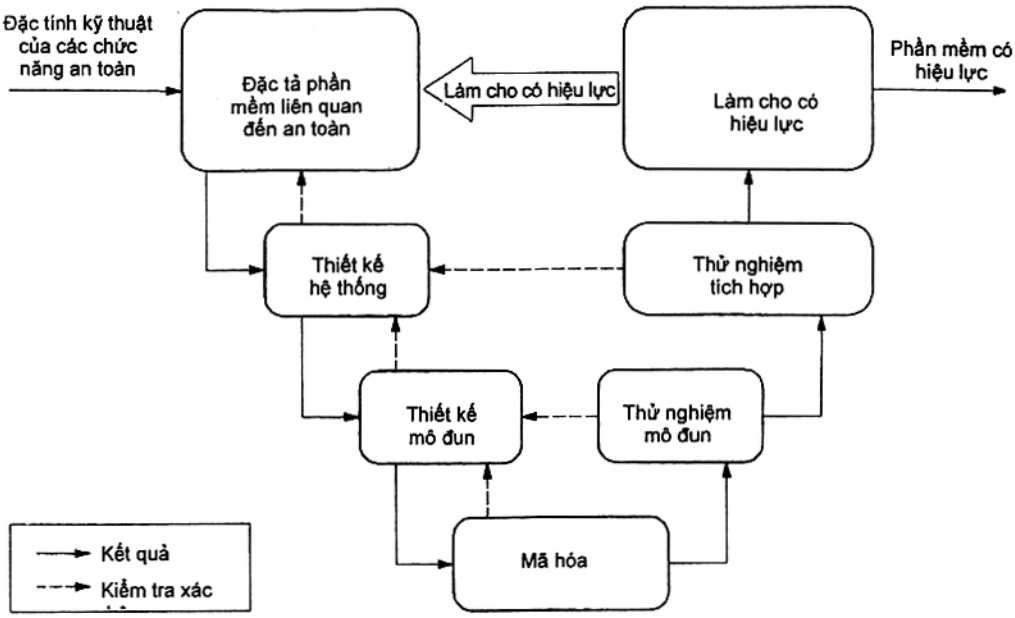
Bảng 7 – Quy trình đơn giản hoá để ước lượng PL mà SRP/CS đạt được

Loại	B	1	2	2	3	3	4
DC_{avg}	Không	Không	Thấp	Trung bình	Thấp	Trung bình	Cao
$MTTF_d$ của mỗi kênh							
Thấp	a	Không bao hàm	a	b	b	c	Không bao hàm
Trung bình	b	Không bao hàm	b	c	c	d	Không bao hàm
Cao	Không bao hàm	c	c	d	d	d	e

4.6 Yêu cầu an toàn của phần mềm

4.6.1 Quy định chung

Phải quan tâm đúng mức tới tất cả các chế độ hoạt động trong vòng đời của phần mềm liên quan đến an toàn được nhúng hoặc ứng dụng để tránh các lỗi phát sinh trong vòng đời của phần mềm (xem Hình 6). Mục tiêu chính của các yêu cầu sau là để có phần mềm đọc được, có thể hiểu được, thử nghiệm được và bảo trì được.



CHÚ THÍCH: Phụ lục J giới thiệu chi tiết hơn về các chế độ hoạt động của vòng đời.

Hình 6 – Mô hình chữ V đơn giản hoá vòng đời an toàn của phần mềm

4.6.2 Phần mềm được nhúng liên quan đến an toàn (SRESW)

Đối với phần mềm được nhúng liên quan đến an toàn (SRESW) dùng cho các bộ phận có mức tính năng yêu cầu (PL_r) từ a đến d phải áp dụng các biện pháp cơ bản sau:

- Vòng đời an toàn của phần mềm có sự kiểm tra và độ hoạt động có hiệu lực, xem Hình 6;
- Lập tài liệu đặc tả và thiết kế;
- Thiết kế cấu trúc, mô đun và mã hoá;
- Kiểm soát các hư hỏng có tính hệ thống (xem G.2);
- Khi sử dụng các biện pháp dựa trên phần mềm để kiểm soát các hư hỏng ngẫu nhiên của phần cứng, kiểm tra sự thực thi đúng;
- Thử nghiệm chức năng, ví dụ, kiểm tra hộp đen;
- Các chế độ hoạt động thích hợp của vòng đời an toàn của phần mềm sau cải tiến.

Đối với phần mềm liên quan đến an toàn được nhứng (SRESW) dùng cho các bộ phận có mức tính năng yêu cầu (PL_r) c hoặc d phải áp dụng các biện pháp bổ sung sau:

- Quản lý dự án và hệ thống quản lý chất lượng có thể so sánh được với, ví dụ, IEC 61508 hoặc TCVN ISO 9001;
- Lập tài liệu bao gồm các chế độ hoạt động có liên quan trong vòng đời an toàn của phần mềm;
- Quản lý cấu hình để định danh tất cả các hạng mục cấu hình và các tài liệu liên quan đến một phiên bản SRESW;
- Đặc tả cấu trúc có các yêu cầu an toàn và thiết kế;
- Sử dụng các ngôn ngữ lập trình thích hợp và các công cụ dựa trên máy tính có độ tin cậy trong sử dụng;
- Lập trình cấu trúc và mô đun, tách biệt trong phần mềm không liên quan đến an toàn, các kích thước mô đun hạn chế với các giao diện được định nghĩa hoàn toàn, sử dụng tiêu chuẩn thiết kế và tiêu chuẩn mã hoá;
- Kiểm tra sự mã hoá bằng bước chuyển đến/xem xét lại có sự phân tích dòng lưu động điều khiển;
- Thử nghiệm chức năng mở rộng, ví dụ, thử nghiệm hộp xám, kiểm nghiệm sự thi hành hoặc mô phỏng;
- Phân tích tác động và các chế độ hoạt động thích hợp của vòng đời an toàn của phần mềm sau cải tiến.

Phần mềm liên quan đến an toàn được nhúng (SRESW) dùng cho các bộ phận có mức tính năng yêu cầu PL_r = e phải tuân theo IEC 61508-3:1998, Điều 7, thích hợp với mức toàn vẹn của an toàn SIL 3. Khi sử dụng tính đa dạng trong đặc tả, thiết kế và mã hoá, đối với hai kênh được sử dụng trong bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) với loại 3 hoặc 4 thì có thể đạt được PL_r = e với các biện pháp nêu trên đối với PL_r c hoặc d.

CHÚ THÍCH 1: Sự mô tả chi tiết các biện pháp như vậy được giới thiệu trong IEC 61508-7:2000.

CHÚ THÍCH 2: Đối với SRESW có tính đa dạng trong thiết kế và mã hoá, đối với các bộ phận được sử dụng trong SRP/CS với loại 3 hoặc 4 thì sự cố gắng trong việc tìm các biện pháp để tránh các hư hỏng có hệ thống có thể được giảm đi bằng cách, ví dụ như xem xét lại các bộ phận của phần mềm chỉ bằng xem xét các khía cạnh về cấu trúc thay cho kiểm tra mỗi dòng mã.

4.6.3 Phần mềm ứng dụng liên quan đến an toàn (SRRASW)

Vòng đời an toàn của phần mềm (xem Hình 6) cũng áp dụng cho phần mềm ứng dụng liên quan đến an toàn (SRASW) (xem Phụ lục J).

Phần mềm ứng dụng liên quan đến an toàn (SRASW) được viết trong ngôn ngữ biến đổi có giới hạn (LVL) và tuân theo các yêu cầu sau có thể đạt được mức tính năng (PL) từ a đến e. Nếu SRASW được

viết bằng ngôn ngữ biến đổi hoàn toàn (FVL) thì phải áp dụng các yêu cầu dùng cho phần mềm liên quan đến an toàn được nhúng (SRESW) và PL có thể đạt được từ a đến e. Nếu một bộ phận của SRASW trong một bộ phận có tác động bất kỳ (ví dụ, do sự cải tiến của nó) đến nhiều chức năng an toàn với PL khác nhau thì phải áp dụng các yêu cầu liên quan đến PL cao nhất. Đối với SRASW dùng cho các bộ phận có PL_r từ a đến e thì phải áp dụng các biện pháp cơ bản sau:

- Phát triển vòng đời có sự kiểm chứng và các chế độ hoạt động có hiệu lực, xem Hình 6;
- Lập tài liệu đặc tả và thiết kế;
- Lập trình cấu trúc và mô đun;
- Kiểm nghiệm chức năng;
- Phát triển các chế độ hoạt động thích hợp sau cải tiến.

Đối với các SRASW dùng cho các bộ phận có PL_r từ c đến e, các biện pháp bổ sung sau có hiệu quả tăng (hiệu quả thấp đối với PL_r là c, hiệu quả trung bình đối với PL_r là d, hiệu quả cao đối với PL_r là e) được yêu cầu và khuyến nghị.

a) Phải xem xét lại đặc tả của phần mềm liên quan đến an toàn (xem Phụ lục J), sẵn có đối với mỗi người có liên quan đến vòng đời và phải có sự mô tả:

   1) Các chức năng an toàn với mức tính năng yêu cầu (Pa_r) và chế độ vận hành kết hợp,

   2) Chuẩn thi hành, ví dụ, các thời gian phản ứng,

   3) Cấu trúc phần cứng với các giao diện tín hiệu ngoài, và

   4) Phát hiện và kiểm soát hư hỏng bên ngoài.

b) Lựa chọn các công cụ, thư viện, ngôn ngữ:

   1) Các công cụ thích hợp có độ tin cậy trong sử dụng; đối với PL = e đạt được với một bộ phận và công cụ của nó, công cụ phải tuân theo tiêu chuẩn an toàn thích hợp; nếu sử dụng hai bộ phận khác nhau với các công cụ khác nhau thì độ tin cậy trong sử dụng có thể là thoả đáng. Phải sử dụng các đặc tính kỹ thuật phát hiện ra các điều kiện có thể gây ra sai số hệ thống (như dữ liệu không tương hợp, sự cấp phát nhập nhằng của bộ nhớ động, các giao diện được gọi không đầy đủ, phép đệ qui, số học con trỏ). Nếu thực hiện việc kiểm tra chủ yếu là trong thời gian biên dịch và không chỉ là tại thời gian chạy. Các công cụ nên củng cố các tập con ngôn ngữ và các hướng dẫn mã hoá hoặc ít nhất là giám sát hoặc hướng dẫn người phát triển sử dụng chúng.

   2) Khi thấy hợp lý và có thể thực hiện được, nên sử dụng các thư viện khối chức năng (FB) có hiệu lực – các thư viện khối chức năng liên quan đến an toàn do nhà sản xuất công cụ cung cấp (rất nên dùng đối với PL = e) hoặc các thư viện khối chức năng ứng dụng riêng có hiệu lực và tuân theo tiêu chuẩn này.

3) Nếu sử dụng tập con ngôn ngữ biến đổi có giới hạn (LVL) đã được chỉnh vị trí thích hợp cho một phương pháp lắp ráp, ví dụ tập con được chấp nhận của các ngôn ngữ IEC 61131-3. Các ngôn ngữ đồ hoạ (ví dụ, biến đồ khối chức năng, biến đồ bậc thang) rất được khuyến nghị sử dụng.

c) Thiết kế phần mềm phải đặc biệt chú ý đến:

1) Các phương pháp nửa chính qui để mô tả các dữ liệu và dòng điều khiển, ví dụ, biểu đồ trạng thái hoặc lưu đồ chương trình,

2) Lập trình cấu trúc và mô đun hầu hết được thực hiện bởi các khối chức năng dẫn xuất từ các thư viện khối chức năng liên quan đến an toàn có hiệu lực,

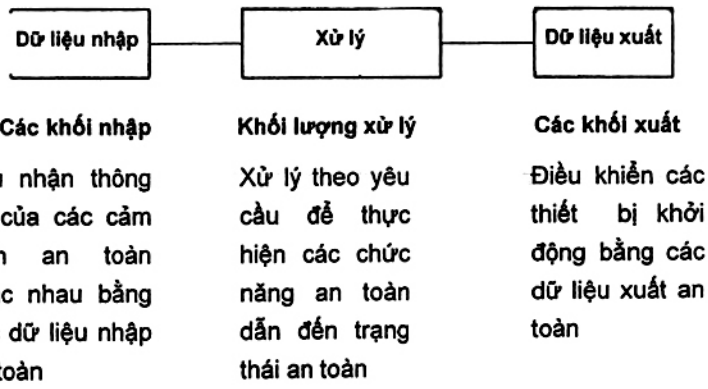
3) Các khối chức năng có kích thước mã hoá hạn chế,

4) Thực hiện mã bên trong khối chức năng có một điểm nhập và một điểm thoát,

5) Mô hình cấu trúc ba bước, khối nhập => khối xử lý => khối xuất (xem Hình 7 và Phụ lục J),

6) Gán một khối xuất an toàn tại chỉ một vị trí của chương trình, và

7) Sử dụng các kỹ thuật để phát hiện hư hỏng bên ngoài và để lập trình bảo vệ bên trong khối nhập, khối xử lý và khối xuất dẫn đến trạng thái an toàn.



Hình 7 – Mô hình cấu trúc chung của phần mềm

d) Khi phần mềm ứng dụng liên quan đến an toàn (SRASW) và phần mềm ứng dụng không liên quan đến an toàn (non-SRASW) được kết hợp trong một bộ phận:

1) SRASW và non – SRASW phải được mã hoá trong các khối chức năng khác nhau có các liên kết dữ liệu đã được định nghĩa;

2) Không được có sự kết hợp logic của các dữ liệu liên quan đến an toàn và các dữ liệu không liên quan đến an toàn dẫn đến việc hạ cấp tính toàn vẹn của các tín hiệu liên quan đến an toàn, ví dụ, kết hợp các tín hiệu liên quan đến an toàn và không liên quan đến an toàn bằng một tín hiệu logic "OR" ở đó kết quả điều khiển các tín hiệu liên quan đến an toàn.

e) Thực thi/mã hóa phần mềm:

1) Mã phải đọc được, có thể hiểu được và thử nghiệm được, và vì lẽ đó nên sử dụng các biến số ký hiệu (thay cho địa chỉ rõ ràng của phần cứng);

2) Phải sử dụng các hướng dẫn mã hoá đã được chấp nhận hoặc chỉnh lý (xem Phụ lục J);

3) Nên sử dụng các kiểm tra tính toàn vẹn và tính hợp lý của dữ liệu (ví dụ, kiểm tra dải) sẵn có trên lớp ứng dụng (lập trình bảo vệ);

4) Nên thử nghiệm mã bằng mô phỏng;

5) Nên kiểm tra bằng việc phân tích và điều khiển dòng dữ liệu đối với PL = d hoặc e.

f) Thử nghiệm:

1) Phương pháp có hiệu lực thích hợp là thử nghiệm trạng thái chức năng và chuẩn thi hành của hộp đen (ví dụ, thi hành đo thời gian);

2) Đối với PL = d hoặc e, nên thực hiện thử nghiệm từ việc phân tích giá trị biên;

3) Cần có kế hoạch thử nghiệm bao gồm các trường hợp thử nghiệm với các chuẩn hoàn tất và công cụ yêu cầu;

4) Thử nghiệm I/O (nhập/xuất) phải bảo đảm rằng các tín hiệu liên quan đến an toàn được sử dụng đúng trong SRASW.

g) Lập tài liệu:

1) Phải lập tài liệu cho toàn bộ vòng đời và các chế độ hoạt động cải tiến;

2) Tài liệu cung cấp phải đầy đủ, có thể dùng được, đọc được và hiểu được;

3) Tài liệu về mã trong văn bản nguồn phải chứa các tiêu đề theo môđun có thực thể hợp thức, mô tả chức năng và mô tả I/O (nhập/xuất), phiên bản và phiên bản của các khối chức năng được sử dụng, các dẫn giải cần thiết của các mạng/lệnh và các dòng thông báo.

h) Kiểm tra xác nhận [2)]

VÍ DỤ: Xem xét lại, kiểm tra, bước chuyển đến hoặc các hoạt động thích hợp khác.

[2)] Kiểm tra xác nhận chỉ cần thiết cho mã ứng dụng đặc biệt và không dùng cho các chức năng thư viện có hiệu lực.

i) Quản lý cấu hình

Các thủ tục và bản sao dự phòng dữ liệu nên được thiết lập để định danh và lưu trữ các tư liệu, các mô đun phần mềm, các kết quả kiểm chứng/tính hiệu lực và cấu hình công cụ có liên quan đến một phiên bản SRASW đặc biệt.

f) Cải tiến

Sau các cải tiến của SRASW, phải thực hiện sự phân tích tác động để bảo đảm sự đặc tả. Phải thực hiện các độ hoạt động thích hợp của vòng đời sau cải tiến. Quyền truy cập các cải tiến phải được kiểm soát và lịch sử cải tiến phải được lập thành tài liệu.

CHÚ THÍCH: Cải tiến không ảnh hưởng đến các hệ thống đã sử dụng.

4.6.4 Tham số hoá dựa trên phần mềm

Tham số hoá dựa trên phần mềm của các tham số liên quan đến an toàn phải được xem là một khía cạnh liên quan đến an toàn trong thiết kế SRP/CS được mô tả trong đặc tả các yêu cầu an toàn của phần mềm. Phải thực hiện sự tham số hoá khi sử dụng một công cụ phần mềm chuyên dụng do nhà cung cấp SRP/CS cung cấp. Công cụ này phải có định danh riêng của nó (tên, phiên bản, v.v...) và phải ngăn ngừa được sự cải tiến không được phép, ví dụ như bằng cách sử dụng một mật khẩu.

Phải duy trì tính toàn vẹn của tất cả các dữ liệu dùng cho tham số hoá. Điều này phải đạt được bằng cách áp dụng các biện pháp để.

- Kiểm soát dải các dữ liệu nhập có hiệu lực,
- Kiểm soát sự làm hỏng dữ liệu trước khi truyền,
- Kiểm soát ảnh hưởng của các sai sót từ quá trình truyền tham số,
- Kiểm soát ảnh hưởng của việc truyền tham số không an toàn, và
- Kiểm soát ảnh hưởng của các lỗi và hư hỏng của phần cứng và phần mềm của công cụ được dùng cho tham số hoá.

Công cụ tham số hoá phải đáp ứng tất cả các yêu cầu đối với SRP/CS theo tiêu chuẩn này. Có thể phải sử dụng một thủ tục đặc biệt để chỉnh đặt các tham số liên quan đến an toàn.

Thủ tục này phải bao gồm sự xác nhận các tham số nhập vào SRP/CS bằng.

- Truyền lại các tham số được cải tiến đến công cụ tham số hoá, hoặc
- Các biện pháp thích hợp khác để xác nhận tính toàn vẹn của các tham số, cũng như sự xác nhận tiếp theo, ví dụ như bởi một người có kỹ năng thích hợp và bằng kiểm tra tự động với việc sử dụng một công cụ tham số hoá.

CHÚ THÍCH 1: Vấn đề nêu trên có ý nghĩa đặc biệt quan trọng khi việc tham số hoá được thực hiện bằng một thiết bị không chuyên dụng (ví dụ, máy tính cá nhân hoặc thiết bị tương đương).

Các mô đun phần mềm dùng để mã hoá / mã hoá trong quá trình truyền/truyền lại và các mô đun phần mềm dùng cho người sử dụng để hình dung các tham số liên quan đến an toàn phải có tính đa dạng trong chức năng để tránh các sai số hệ thống.

Sự cung cấp dữ liệu tham số hoá dựa trên phần mềm phải chỉ ra dữ liệu được sử dụng (ví dụ, bộ các tham số được xác định trước) và thông tin cần thiết để định danh các tham số được xác định trước) và thông tin cần thiết để định danh các tham số gắn liền với SRP/CS, người thực hiện việc tham số hoá cùng với các thông tin có liên quan khác như ngày tham số hoá.

Phải áp dụng các hoạt động kiểm tra sau đối với quá trình tham số hoá dựa trên phần mềm:

- Kiểm tra sự chỉnh đặt đúng, đối với mỗi tham số liên quan đến an toàn (các giá trị nhỏ nhất, lớn nhất và đại diện);
- Kiểm tra xác minh rằng các tham số liên quan đến an toàn đã được kiểm về tính hợp lý, ví dụ như bằng cách sử dụng các giá trị không hợp lệ, v.v...;
- Kiểm tra xác minh rằng sự cải tiến không được phép đối với các tham số liên quan đến an toàn đã được ngăn ngừa;
- Kiểm tra xác minh rằng các dữ liệu/tín hiệu dùng cho tham số hoá đã được tạo ra và xử lý theo cách các lỗi không thể dẫn đến việc làm mất đi chức năng an toàn;

CHÚ THÍCH 2: Vấn đề nêu trên có ý nghĩa đặc biệt quan trọng khi việc tham số hoá được thực hiện bằng một thiết bị không chuyên dụng (ví dụ, máy tính cá nhân hoặc thiết bị tương đương).

4.7 Kiểm tra bảo đảm rằng PL đạt được đáp ứng PL_r

Đối với mỗi chức năng an toàn riêng, mức tính năng (PL) của bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) có liên quan phải thích hợp với mức tính năng yêu cầu (PL_r) được xác định theo 4.3 (xem Hình 3). Nếu không đạt được yêu cầu này thì cần thiết phải lặp lại quá trình được mô tả trên Hình 3.

PL của SRP/CS khác nhau, là một phần của chức năng an toàn, phải bằng hoặc lớn hơn mức tính năng yêu cầu (PL_r) của chức năng an toàn này.

4.8 Khía cạnh êgônômi của thiết kế

Giao diện giữa người vận hành và các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) phải được thiết kế và thực hiện sao cho không có người nào bị nguy hiểm trong toàn bộ qua trình sử dụng máy theo hướng dẫn và sử dụng máy sai hợp lý thấy trước được [xem TCVN 7383-2 (ISO 12100-2), EN 6114-1, ISO 9355-2, ISO 9355-3, EN 1005-3, IEC 60204-1:2000, Điều 10, IEC 60447 và IEC 61310].

Phải sử dụng các nguyên tắc êgônômi để cho máy và hệ thống điều khiển, bao gồm cả các bộ phận liên quan đến an toàn được sử dụng dễ dàng và người vận hành không bị lôi cuốn vào các thao tác nguy hiểm.

Cần áp dụng các yêu cầu an toàn đối với các nguyên tắc êgônômi phải tuân theo được giới thiệu TCVN 7383-2 (ISO 12100-2).

5 Chức năng an toàn

5.1 Đặc điểm của các chức năng an toàn

Điều này đưa ra bản danh sách và nội dung chi tiết của các chức năng an toàn do các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) cung cấp. Người thiết kế (hoặc người làm tiêu chuẩn loại C) phải tính đến các yêu cầu cần thiết để đạt được các biện pháp an toàn yêu cầu của hệ thống điều khiển đối với các ứng dụng riêng.

VÍ DỤ: Chức năng dừng liên quan đến an toàn, ngăn ngừa sự khởi động bất ngờ, chức năng chỉnh đặt lại bằng tay, chức năng tạm ngừng, chức năng giữ cho chạy.

CHÚ THÍCH: Các hệ thống điều khiển máy cung cấp các chức năng vận hành và/hoặc an toàn. Các chức năng vận hành (ví dụ, khởi động, dừng bình thường) cũng có thể là các chức năng an toàn, nhưng điều này có thể được xác minh chỉ sau khi đã thực hiện việc đánh giá đầy đủ rủi ro trên máy.

Bảng 8 và Bảng 9 liệt kê một số chức năng an toàn điển hình, một số đặc tính của chúng và các tham số liên quan đến an toàn, trong khi có sự tham chiếu các tiêu chuẩn quốc tế khác có các yêu cầu liên quan đến chức năng, đặc tính hoặc tham số an toàn. Người thiết kế (hoặc người làm tiêu chuẩn loại C) phải bảo đảm rằng tất cả các yêu cầu áp dụng thoả mãn đối với các chức năng an toàn có liên quan được liệt kê trong bảng.

Các yêu cầu bổ sung được lập ra trong điều này dùng cho một số đặc tính của chức năng an toàn.

Khi cần thiết, các yêu cầu đối với các đặc tính và chức năng an toàn phải được sửa lại cho thích hợp trong sử dụng với các nguồn năng lượng khác nhau.

Vì phần lớn các tiêu chuẩn tham chiếu trong các Bảng 8 và Bảng 9 là các tiêu chuẩn về điện cho nên các yêu cầu áp dụng sẽ cần được sửa lại cho thích hợp trong trường hợp sử dụng các công nghệ khác (ví dụ, thuỷ lực, khí nén).

Bảng 8 - Một số tiêu chuẩn quốc tế áp dụng cho các chức năng an toàn điển hình của máy và các đặc tính của chúng

Chức năng an toàn/đặc tính	Yêu cầu			Xem thông tin bổ sung trong:
	TCVN 7384-1 (ISO 13849-1)	TCVN 7383-1:2004 (ISO 12100-1:2003)	TCVN 7383-2:2004 (ISO 12100-2:2003)	
Chức năng dừng an toàn được bắt đầu bằng bộ phận bảo vệ [a]	5.2.1	3.2.6.8	4.11.3	IEC 60204-1:2005, 9.2.2, 9.2.5.3, 9.2.5.5
Chức năng chỉnh đặt lại bằng tay	5.2.2	–	–	IEC 60204-1:2005, 9.2.5.3, 9.2.5.4
Chức năng khởi động/khởi động lại	5.2.3	–	4.11.3, 4.11.4	IEC 60204-1:2005, 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6
Chức năng điều khiển cục bộ	5.2.4	–	4.11.8, 4.11.10	IEC 60204-1:2005, 10.1.5
Chức năng tạm ngừng	5.2.5	–	–	–
Chức năng giữ cho chạy		–	–	IEC 60204-1:2005, 9.2.6.1
Chức năng cho phép của thiết bị		–	–	IEC 60204-1:2005, 9.2.6.3, 10.9
Ngăn ngừa khởi động bất ngờ	–	–	4.11.4	TCVN 7300 (ISO 14118), IEC 60204-1:2005, 54
Giải thoát và cứu người bị kẹt	–	–	5.5.3	–
Chức năng cách ly và tiêu tán năng lượng	–	–	5.5.4	TCVN 7300 (ISO 14118), IEC 60204-1:2005, 5.3, 6.3.1
Các dạng điều khiển và chọn dạng điều khiển	–	–	4.11.8, 4.11.10	IEC 60204-1:2005, 9.2.3, 9.2.4
Tương tác giữa các bộ phận liên quan đến an toàn khác nhau của các hệ thống điều khiển	–	–	4.11.1 (Câu cuối cùng)	IEC 60204-1:2005, 9.3.4

Bảng 8 (Kết thúc)

Chức năng an toàn/đặc tính	Yêu cầu			Xem thông tin bổ sung trong:
	TCVN 7384-1 (ISO 13849-1)	TCVN 7383-1:2004 (ISO 12100-1:2003)	TCVN 7383-2:2004 (ISO 12100-2:2003)	
Giám sát và tham số hoá các giá trị nhập liên quan đến an toàn	4.6.4	–	–	–
Chức năng dừng khẩn cấp[b]	–	–	5.5.2	TCVN 6719 (ISO 13850), IEC 60204-1 : 2005, 9.2.5.4
[a] Bao gồm các bộ phận bảo vệ khoá liên động và các thiết bị hạn chế (ví dụ, vượt tốc, quá nhiệt độ, quá áp suất). [b] Đối với các biện pháp bảo vệ bổ sung, xem TCVN 7383-1:2004 (ISO 12100-1:2003).				

Bảng 9 - Một số tiêu chuẩn quốc tế cho các yêu cầu về các chức năng an toàn và các tham số liên quan an toàn

Chức năng an toàn/tham số liên quan đến an toàn	Yêu cầu		Xem thông tin bổ sung trong:
	TCVN 7384-1 (ISO 13849-1)	TCVN 7383-2:2004 (ISO 12100-2:2003)	
Thời gian đáp ứng	5.2.6		TCVN 7386:2004 (ISO 13855:2000), 3.2, A.3, A.4
Tham số liên quan đến an toàn như tốc độ, nhiệt độ hoặc áp suất	5.2.7	4.11.8.e)	IEC 60204-1:2005, 7.1, 9.3.2, 9.3.4
Độ dao động, tổn thất và sự phục hồi các nguồn năng lượng	5.2.8	4.11.8.e)	IEC 60204-1:2005, 4.3, 7.1, 7.5
Chỉ báo và báo động (cảnh báo)	–	4.8	ISO 7731 ISO 11428 ISO 11429 IEC 61310-1 IEC 60204-1:2005, 10.3, 10.4 IEC 61131 IEC 62061

Khi nhận dạng và quy định các chức năng an toàn, ít nhất phải xem xét đến các yêu cầu sau:

a) Các kết quả đánh giá rủi ro đối với mỗi mối nguy hiểm hoặc tình trạng nguy hiểm riêng;

b) Các đặc tính làm việc của máy, bao gồm

- Sử dụng máy theo hướng dẫn (bao gồm cả sử dụng sai hợp lý thấy trước),
- Các chế độ vận hành (ví dụ, chế độ cục bộ, chế độ tự động, các chế độ liên quan đến một vùng hoặc một bộ phận của máy),
- Thời gian của chu kỳ, và
- Thời gian đáp ứng;

c) Hoạt động khẩn cấp;

d) Mô tả sự tương tác của các quá trình gia công khác nhau và các hoạt động bằng tay (sửa chữa, chỉnh đặt, làm sạch, khắc phục sự trục trặc v.v...);

e) Tình trạng của máy cần đạt tới hoặc cần được ngăn ngừa khi sử dụng một chức năng an toàn;

f) Điều kiện của máy (ví dụ, chế độ vận hành) ở đó máy hoạt động được hoặc bị hư hỏng;

g) Tần suất vận hành;

h) Sự ưu tiên của các chức năng có thể hoạt động được đồng thời và có thể dẫn đến hoạt động đối lập nhau.

5.2 Nội dung chi tiết của các chức năng an toàn

5.2.1 Chức năng dừng liên quan đến an toàn

Ngoài các yêu cầu của Bảng 8, cần áp dụng yêu cầu sau.

Một chức năng dừng liên quan đến an toàn (ví dụ, được bắt đầu bằng một thiết bị bảo vệ) phải đưa máy về trạng thái an toàn ngay sau khi được khởi động. Sự dừng này được ưu tiên so với sự dừng vì lý do vận hành.

Khi một nhóm máy làm việc có sự phối hợp với nhau thì phải có phương tiện báo hiệu sự giảm sát và/hoặc báo hiệu cho các máy khác rằng đã có một trạng thái dừng.

CHÚ THÍCH: Một chức năng dừng liên quan đến an toàn có thể gây ra các vấn đề vận hành và khởi động lại khó khăn, ví dụ, trong ứng dụng hàn hồ quang. Để giảm khả năng dẫn đến thất bại của chức năng dừng này, có thể thực hiện trước sự dừng vì lý do vận hành để kết thúc nguyên công hiện thời và chuẩn bị cho sự khởi động lại nhanh và dễ dàng từ vị trí dừng (ví dụ, không có bất cứ sự thiệt hại nào đối với sản xuất). Có thể có một giải pháp là sử dụng thiết bị khoá liên động có sự khoá bảo vệ ở đó sự khoá bảo vệ được nhả ra khi chu kỳ đã đạt tới một điểm xác định để khởi động lại dễ dàng.

5.2.2 Chức năng chỉnh đặt lại bằng tay

Ngoài các yêu cầu của Bảng 8, cần áp dụng yêu cầu sau:

Sau một lệnh dừng được bắt đầu bởi một bộ phận an toàn, trạng thái dừng phải được duy trì tới khi có các điều kiện an toàn cho khởi động lại.

Việc thiết lập lại chức năng an toàn bằng cách chỉnh đặt lại bộ phận an toàn đã huỷ bỏ lệnh dừng. Nếu được chỉ dẫn trong đánh giá rủi ro thì việc xoá bỏ lệnh dừng này phải được xác nhận bằng một tác động bằng tay có chủ định và riêng biệt (chỉnh đặt lại bằng tay). Chức năng chỉnh đặt lại bằng tay phải:

- Được cung cấp thông qua một cơ cấu được vận hành bằng tay và riêng biệt trong bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS),
- Chỉ đạt được nếu tất cả các chức năng an toàn và các thiết bị bảo vệ hoạt động,
- Không khởi xướng chuyển động hoặc tình trạng nguy hiểm bởi chính chức năng chỉnh đặt lại bằng tay này,
- Được thực hiện bằng tác động có chủ định,
- Làm cho hệ thống điều khiển có khả năng chấp nhận một lệnh khởi động riêng biệt,
- Chỉ được chấp nhận bằng nhả khớp (ngắt) cơ cấu tác động khỏi vị trí kích hoạt của nó.

Mức tính năng của các bộ phận liên quan đến an toàn cung cấp chức năng chỉnh đặt lại bằng tay phải được lựa chọn sao cho việc đưa vào chức năng chỉnh đặt lại bằng tay không làm giảm đi mức an toàn yêu cầu của chức năng an toàn có liên quan.

Cơ cấu tác động để chỉnh đặt lại phải được bố trí ngoài vùng nguy hiểm và ở một vị trí an toàn, dễ nhìn thấy để kiểm tra bảo đảm rằng không có người ở trong vùng nguy hiểm.

Khi không nhìn thấy vùng nguy hiểm một cách đầy đủ, cần có một quy trình chỉnh đặt lại đặc biệt.

CHÚ THÍCH: Có một giải pháp nữa là sử dụng một cơ cấu tác động thứ hai để chỉnh đặt lại. Chức năng chỉnh đặt lại được bắt đầu trong vùng nguy hiểm bởi cơ cấu tác động thứ nhất kết hợp với cơ cấu tác động thứ hai để chỉnh đặt lại được bố trí ngoài vùng nguy hiểm (gần thiết bị bảo vệ). Phương pháp chỉnh đặt lại này cần được thực hiện trong một thời gian hạn chế trước khi hệ thống điều khiển nhận một lệnh khởi động riêng biệt.

5.2.3 Chức năng khởi động/khởi động lại

Ngoài các yêu cầu của Bảng 8, cần áp dụng yêu cầu sau.

Sự khởi động lại chỉ xảy ra một cách tự động nếu không có tình trạng nguy hiểm. Đặc biệt là đối với các thiết bị bảo vệ khoá liên động có một chức năng khởi động, áp dụng TCVN 7383-2:2004 (ISO 12100-2:2003), trong 5.3.2.5. Các yêu cầu này đối với khởi động và khởi động lại phải được áp dụng cho các máy được điều khiển từ xa.

CHÚ THÍCH: Một tín hiệu phản hồi của bộ cảm biến đến hệ thống điều khiển có thể bắt đầu sự khởi động lại tự động.

VÍ DỤ: Trong các hoạt động của máy tự động, các tín hiệu phản hồi của bộ cảm biến đến hệ thống điều khiển thường được sử dụng để điều khiển tiến trình công nghệ. Nếu chi tiết gia công rồi ra khỏi vị trí thì tiến trình công nghệ dừng lại. Nếu sự giám sát của thiết bị bảo vệ khoá liên động không cao hơn sự điều khiển quá trình tự động thì có thể có nguy hiểm cho sự khởi động lại máy trong khi người vận hành điều chỉnh lại chi tiết gia công. Do đó không cho phép khởi động lại được điều khiển từ xa tới khi thiết bị bảo vệ được đóng lại và người vận hành rời khỏi vùng nguy hiểm. Sự đóng góp vào sự phòng ngừa khởi động bất ngờ do hệ thống điều khiển cung cấp phụ thuộc vào kết quả của việc đánh giá rủi ro.

5.2.4 Chức năng điều khiển cục bộ

Ngoài các yêu cầu của Bảng 8, cần áp dụng các yêu cầu sau.

Khi một máy được điều khiển cục bộ, ví dụ bằng cơ cấu điều khiển xách tay hoặc treo, phải áp dụng các yêu cầu sau:

- Phương tiện để chọn điều khiển cục bộ phải được bố trí ngoài vùng nguy hiểm;
- Chỉ có thể bắt đầu các tình trạng nguy hiểm bằng sự điều khiển cục bộ trong một vùng do sự đánh giá rủi ro xác định;
- Sự chuyển mạch giữa điều khiển cục bộ và điều khiển chính không được tạo ra tình trạng nguy hiểm.

5.2.5 Chức năng tạm ngừng

Ngoài các yêu cầu của Bảng 8, cần áp dụng yêu cầu sau.

Sự tạm ngừng không được làm cho bất cứ người nào bị phơi ra trước tình trạng nguy hiểm. Trong quá trình tạm ngừng phải có các điều kiện an toàn do các phương tiện khác cung cấp.

Khi kết thúc sự tạm ngừng, phải khôi phục tất cả các chức năng an toàn của các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS).

Mức tính năng của các bộ phận liên quan đến an toàn cung cấp chức năng tạm ngừng phải được lựa chọn sao cho sự đưa vào chức năng tạm ngừng không làm suy giảm mức an toàn yêu cầu của chức năng an toàn có liên quan.

CHÚ THÍCH: Trong một số ứng dụng cần có một tín hiệu chỉ báo sự tạm dừng.

5.2.6 Thời gian đáp ứng

Ngoài các yêu cầu của Bảng 9, cần áp dụng yêu cầu sau.

Phải xác định thời gian đáp ứng của bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) khi sự đánh giá rủi ro của SRP/CS chỉ ra rằng yêu cầu này là cần thiết (xem Điều 11).

CHÚ THÍCH: Thời gian đáp ứng của hệ thống điều khiển là một phần của toàn bộ thời gian đáp ứng của máy có thể ảnh hưởng đến thiết kế bộ phận liên quan đến an toàn, ví dụ, sự cần thiết phải cung cấp một hệ thống phanh.

5.2.7 Tham số liên quan đến an toàn

Ngoài các yêu cầu của Bảng 9, cần áp dụng các yêu cầu sau.

Khi các tham số liên quan đến an toàn ví dụ như vị trí, tốc độ, nhiệt độ hoặc áp suất, sai lệch so với các giới hạn hiện thời thì hệ thống điều khiển phải bắt đầu các biện pháp thích hợp (ví dụ, tác động dừng, tín hiệu cảnh báo, báo động).

Nếu các sai sót trong việc nhập vào bằng tay các dữ liệu liên quan đến an toàn trong các hệ thống điện tử lập trình có thể dẫn đến một tình trạng nguy hiểm thì phải có một hệ thống kiểm tra dữ liệu trong hệ thống điều khiển liên quan đến an toàn, ví dụ, kiểm các giới hạn, các giá trị nhập định dạng và/hoặc logic.

5.2.8 Độ dao động, tổn thất và phục hồi các nguồn năng lượng

Ngoài các yêu cầu của Bảng 9, cần áp dụng yêu cầu sau.

Khi xảy ra độ dao động trong các mức năng lượng vượt ra ngoài phạm vi thiết kế cho vận hành, bao gồm cả tổn thất của sự cung cấp năng lượng thì bộ phận an toàn của hệ thống điều khiển (SRP/CS) phải tiếp tục cung cấp hoặc bắt đầu tín hiệu xuất để có thể duy trì các bộ phận khác của hệ thống máy ở trạng thái an toàn.

6 Các loại và quan hệ của chúng đến $MTTF_d$ của mỗi kênh, DC_{avg} và CCF

6.1 Quy định chung

Bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) phải theo các yêu cầu của một hoặc nhiều loại trong năm loại được quy định trong 6.2.

Các loại là các tham số cơ bản dùng để đạt được mức tính năng (PL) riêng. Chúng biểu thị trạng thái yêu cầu của SRP/CS về khả năng chống lại các lỗi dựa trên các xem xét thiết kế được mô tả trong Điều 4.

Loại B là loại cơ bản. Sự xuất hiện của một lỗi có thể dẫn đến sự mất chức năng an toàn. Trong loại 1 đã được cải tiến, khả năng chống lại các lỗi phần lớn đạt được bằng cách lựa chọn và ứng dụng các bộ phận. Trong các loại 2, 3 và 4, tính năng đã được cải tiến đối với một chức năng an toàn quy định phần lớn đạt được bằng cách cải tiến cấu trúc của SRP/CS. Trong loại 2, yêu cầu này được quy định bằng việc kiểm tra định kỳ để bảo đảm rằng chức năng an toàn quy định đang được thực hiện. Trong

các loại 3 và 4, yêu cầu này được quy định bằng việc bảo đảm rằng một lỗi sẽ không dẫn đến làm mất chức năng an toàn. Trong loại 4 và trong cả loại 3 khi thấy thích hợp, các lỗi này sẽ được phát hiện. Trong loại 4, khả năng chống lại sự tích luỹ các lỗi sẽ được quy định. Bảng 10 đưa ra sự mô tả ngắn gọn các loại SRP/CS, các yêu cầu và trạng thái của hệ thống trong trường hợp có lỗi.

Khi xem xét các nguyên nhân của hư hỏng trong một số bộ phận, có thể loại trừ một số lỗi (xem Điều 7).

Sự lựa chọn một loại cho một SRP/CS cụ thể phụ thuộc chủ yếu vào:

- Sự giảm rủi ro đạt được bằng chức năng an toàn mà bộ phận này đã đóng góp;
- Mức tính năng yêu cầu (PL_r);
- Các công nghệ sử dụng;
- Sự tăng lên của rủi ro trong trường hợp có một lỗi trong bộ phận;
- Các khả năng tránh lỗi trong bộ phận (các lỗi có hệ thống);
- Xác suất xảy ra lỗi trong bộ phận và các tham số có liên quan;
- Thời gian trung bình tới khi hư hỏng nguy hiểm ($MTTF_d$);
- Vùng chẩn đoán (DC) và
- Lỗi do nguyên nhân chung (CCF) trong trường hợp của các loại 2, 3 và 4.

6.2 Đặc tính kỹ thuật của các loại

6.2.1 Quy định chung

Mỗi bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) phải tuân theo các yêu cầu của loại có liên quan, xem 6.2.3 đến 6.2.7.

Các cấu trúc sau đáp ứng các yêu cầu của loại tương ứng.

Các Hình vẽ sau không phải là các ví dụ nhưng chỉ ra các cấu trúc chung. Thường có thể có sai lệch so với các cấu trúc này, nhưng bất cứ sai lệch nào cũng phải được chứng minh bằng các công cụ phân tích thích hợp (ví dụ, mô hình Markov, phân tích lỗi dạng cây) sao cho hệ thống đáp ứng mức tính năng yêu cầu (PL_r).

Các cấu trúc được thiết kế không thể chỉ được xem như các sơ đồ mạch nhưng có thể được xem như các sơ đồ logic. Đối với các loại 3 và 4, điều này có nghĩa là không phải tất cả các bộ phận đều cần phải được làm dư thừa nhưng phải có các biện pháp làm dư thừa để bảo đảm rằng một lỗi không thể dẫn đến việc làm mất chức năng an toàn.

Các đường và mũi tên trên Hình từ 8 đến Hình 12 biểu thị các phương tiện nối và các phương tiện chẩn đoán logic.

6.2.2 Cấu trúc thiết kế

Cấu trúc của một SRP/CS là một đặc trưng chủ chốt có ảnh hưởng lớn đến PL. Dẫu rằng tính đa dạng của các cấu trúc có thể là khá cao nhưng các khái niệm cơ bản thường là giống nhau. Vì vậy, hầu hết các cấu trúc có mặt trong lĩnh vực máy móc có thể được vẽ sơ đồ cho một trong các loại. Đối với mỗi loại, cách trình bày điển hình là vẽ sơ đồ khối liên quan đến an toàn. Các sơ đồ này được gọi là các cấu trúc thiết kế và được đưa vào nội dung văn bản của mỗi loại trong các loại sau.

Điều quan trọng là PL chỉ ra trên Hình 5, phụ thuộc vào loại, $MTTF_d$ của mỗi kênh và DC_{avg}, được dựa trên các cấu trúc thiết kế. Nếu sử dụng Hình 5 để dự tính PL thì cấu trúc của SRP/CS nên được thể hiện tương đương với cấu trúc thiết kế của loại được yêu cầu. Các thiết kế đáp ứng được các đặc tính của loại tương ứng thường là tương đương với cấu trúc thiết kế tương ứng của loại.

CHÚ THÍCH: Trong một số trường hợp xuất hiện từ một giải pháp kỹ thuật riêng hoặc được xác định bởi một tiêu chuẩn loại C thì chất lượng liên quan đến an toàn của SRP/CS chỉ có thể được yêu cầu bởi một loại không có PL_r bổ sung. Đối với các trường hợp riêng này, an toàn được cung cấp một cách đặc biệt bằng cấu trúc và không áp dụng các yêu cầu đối với MTTF, DC, CCF.

6.2.3 Loại B

SRP/CS tối thiểu phải được thiết kế, cấu trúc, lựa chọn, lắp ráp và phối hợp theo các tiêu chuẩn có liên quan và sử dụng các nguyên tắc an toàn cơ bản cho ứng dụng riêng để chịu được:

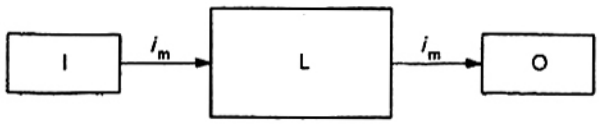
- Các ứng suất làm việc yêu cầu, ví dụ, độ tin cậy về khả năng và tần suất ngắt mạch;
- Ảnh hưởng của vật liệu được gia công, ví dụ, các chất tẩy rửa trong máy giặt, và
- Các ảnh hưởng bên ngoài khác có liên quan, ví dụ, rung cơ học, nhiễu điện từ, sự gián đoạn hoặc nhiễu loạn trong cung cấp năng lượng hoặc điện năng.

Không có vùng chẩn đoán (DC_{avg} = không) trong các hệ thống loại B và MTT F_d của mỗi kênh có thể ở dưới mức trung bình. Trong các cấu trúc này (thường là các hệ thống một kênh) không xem xét đến lỗi do nguyên nhân chung (CCF).

Giá trị lớn nhất của PL đạt được với loại B là PL = b.

CHÚ THÍCH: Khi xảy ra một lỗi thì nó có thể dẫn đến việc mất đi chức năng an toàn.

Các yêu cầu riêng đối với tính tương thích điện từ được cho trong các tiêu chuẩn sản phẩm có liên quan, ví dụ, IEC 61800-3 dùng cho các hệ thống dẫn động điện năng. Đối với an toàn chức năng của SRP/CS, đặc biệt là các yêu cầu về sự không bị ảnh hưởng là có liên quan. Nếu không có tiêu chuẩn sản phẩm thì ít nhất là nên tuân theo các yêu cầu về sự không bị ảnh hưởng của IEC 61000-6-2.



CHÚ DẪN:

i_m phương tiện nối

I thiết bị nhập, ví dụ, cảm biến

L logic

O thiết bị xuất, ví dụ công tắc tơ chính

Hình 8 – Cấu trúc thiết kế đối với loại B

6.2.4 Loại 1

Đối với loại 1, phải áp dụng các yêu cầu tương tự như các yêu cầu theo 6.2.3 đối với loại B. Ngoài ra phải áp dụng yêu cầu sau.

Bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) của loại 1 phải được thiết kế và cấu trúc khi sử dụng các bộ phận và các nguyên tắc an toàn đã quen và đáng tin cậy [xem TCVN 7384-2 (ISO 13849-2)].

Một "bộ phận đã quen và đáng tin cậy" đối với một ứng dụng liên quan đến an toàn là một bộ phận:

a) Đã được sử dụng rộng rãi trong quá khứ có kết quả tốt trong các ứng dụng tương tự, hoặc

b) Được chế tạo và kiểm tra khi sử dụng các nguyên tắc chứng minh được sự thích hợp và độ tin cậy của nó đối với các ứng dụng liên quan đến an toàn.

Các bộ phận và nguyên tắc an toàn mới phát triển có thể được xem là tương đương với các "bộ phận đã quen và đáng tin cậy" nếu chúng đáp ứng được các điều kiện b).

Việc quyết định chấp nhận một bộ phận cụ thể là "bộ phận đã quen và đáng tin cậy" phụ thuộc vào ứng dụng.

CHÚ THÍCH 1: Các bộ phận điện tử phức hợp (ví dụ, PLC, bộ vi xử lý, mạch tích hợp ứng dụng riêng không thể được xem là tương đương với "bộ phận đã quen và đáng tin cậy".

Thời gian trung bình tới khi hư hỏng nguy hiểm ($MTTF_d$) của mỗi kênh phải cao.

Giá trị lớn nhất của PL đạt được với loại 1 là PL = c.

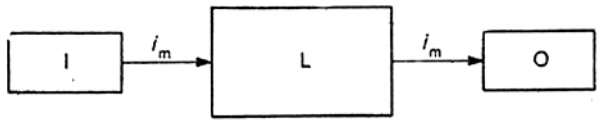
CHÚ THÍCH 2: Không có vùng chẩn đoán (DC_{avg} = không) trong các hệ thống loại 1. Trong các cấu trúc này (các hệ thống một kênh) không xem xét đến lỗi do nguyên nhân chung (CCF).

CHÚ THÍCH 3: Khi xảy ra một lỗi thì nó có thể dẫn đến việc mất đi chức năng an toàn. Tuy nhiên, $MTTF_d$ của mỗi kênh trong loại 1 cao hơn trong loại B. Do đó, sự mất đi chức năng an toàn rất có thể ít đi.

Điều quan trọng là phải có sự phân biệt rõ ràng giữa "bộ phận đã quen và đáng tin cậy" và "sự ngăn chặn lỗi" (xem Điều 7). Phẩm chất của một bộ phận được xem là đã quen và đáng tin cậy phụ thuộc

vào ứng dụng của nó. Ví dụ, một công tắc vị trí có các tiếp điểm mở cưỡng bức có thể được xem là đã quen và đáng tin cậy đối với một máy công cụ, trong khi đồng thời là không thích hợp cho ứng dụng trong công nghiệp thực phẩm – trong công nghiệp sữa chẳng hạn, công tắc này sẽ bị phá huỷ bởi axit của sữa sau một ít tháng. Sự ngăn chặn lỗi có thể dẫn đến một giá trị PL rất cao nhưng cần áp dụng các biện pháp thích hợp để cho phép sự ngăn chặn lỗi này trong toàn bộ tuổi thọ của thiết bị. Để bảo đảm yêu cầu này, có thể cần đến các biện pháp bổ sung bên ngoài hệ thống điều khiển. Trong trường hợp một công tắc vị trí, một số ví dụ về các loại biện pháp này là:

- Phương pháp để cố định chắc chắn công tắc sau khi điều chỉnh;
- Phương tiện để cố định chắc chắn cam;
- Phương tiện để bảo đảm độ ổn định ngang của cam;
- Phương tiện để tránh hành trình quá đà của công tắc vị trí, ví dụ, độ bền lắp ráp thích hợp của bộ giảm xóc và bất cứ cơ cấu chỉnh thẳng hàng nào, và
- Phương tiện bảo vệ chống hư hỏng từ bên ngoài.



CHÚ DẪN:

i_m phương tiện nối

I thiết bị nhập, ví dụ, cảm biến

L logic

O thiết bị xuất, ví dụ, công tắc tơ chính

Hình 9 – Cấu trúc lựa chọn đối với loại 1

6.2.5 Loại 2

Đối với loại 2, phải áp dụng các yêu cầu tương tự như các yêu cầu theo 6.2.3 đối với loại B. Phải tuân theo các "nguyên tắc an toàn đã quen và đáng tin cậy" theo 6.2.4. Ngoài ra cần áp dụng yêu cầu sau.

Bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) loại 2 phải được thiết kế sao cho chức năng của nó được kiểm tra ở các khoảng thời gian thích hợp bằng hệ thống điều khiển của máy. Phải thực hiện việc kiểm tra chức năng an toàn:

- Lúc khởi động máy, và

- Trước khi bắt đầu bất cứ tình trạng nguy hiểm nào, ví dụ, khởi động một chu kỳ mới, khởi động các chuyển động khác, và/hoặc theo định kỳ quá trình hoạt động (vận hành) chỉ ra rằng việc kiểm tra này là cần thiết.

Sự bắt đầu của phép kiểm tra này có thể là tự động. Bất cứ phép kiểm tra chức năng an toàn nào cũng phải:

- Cho phép hoạt động nếu không phát hiện được lỗi, hoặc
- Tạo ra một tín hiệu xuất để bắt đầu tác động điều khiển thích hợp, nếu phát hiện ra một lỗi.

Nếu có thể, tín hiệu xuất này phải bắt đầu một trạng thái an toàn. Trạng thái an toàn này phải được duy trì tới khi xảy ra lỗi. Khi không thể bắt đầu một trạng thái an toàn, (ví dụ, hàn tiếp điểm trong cơ cấu chuyển mạch dừng) thì tín hiệu xuất phải đưa ra sự cảnh báo nguy hiểm.

Đối với cấu trúc lựa chọn loại 2 như đã chỉ ra trên Hình 10, việc tính toán $MTTF_d$ và DC_{avg} chỉ cần tiính đến các khối của kênh chức năng (nghĩa là I, L và O trên Hình 10) và không tính đến các khối của kênh thử nghiệm (nghĩa là TE và TTE trên Hình 10).

Vùng chẩn đoán (DC_{avg}) của tổng SRP/CS bao gồm sự phát hiện lỗi phải thấp. $MTTF_d$ của mỗi kênh phải là thấp – đến – cao tuỳ thuộc vào mức tính năng yêu cầu (PL_r). Phải áp dụng các biện pháp tránh lỗi do nguyên nhân chung (CCF) (xem Phụ lục F).

Bản thân phép kiểm tra không được dẫn đến tình trạng nguy hiểm (ví dụ do sự tăng lên của thời gian đáp ứng). Thiết bị kiểm tra có thể gắn liền hoặc tách rời khỏi bộ phận liên quan đến an toàn cung cấp chức năng an toàn.

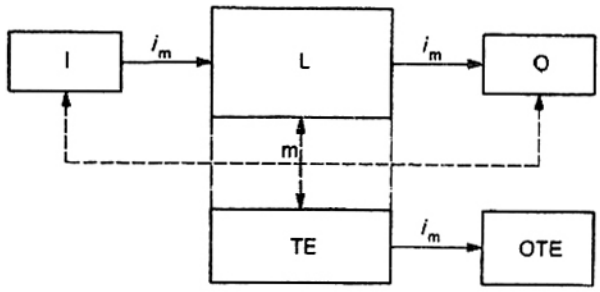
Giá trị lớn nhất của PL đạt được với loại 2 là PL = d.

CHÚ THÍCH 1: Loại 2 không áp dụng được trong một số trường hợp bởi vì không thể áp dụng phép kiểm tra chức năng an toàn cho tất cả các bộ phận.

CHÚ THÍCH 2: Trạng thái của hệ thống loại 2 không cho phép.

- Xảy ra một lỗi có thể dẫn đến việc mất đi chức năng an toàn giữa các kiểm tra;
- Mất chức năng an toàn được phát hiện bằng kiểm tra.

CHÚ THÍCH 3: Nguyên tắc dùng cho phê duyệt một chức năng loại 2 là các điều kiện kỹ thuật được chấp nhận, và, ví dụ như việc lựa chọn tần suất kiểm tra có thể làm giảm xác suất xảy ra một tình trạng nguy hiểm.



Các nét đứt biểu thị sự phát hiện lỗi thực tế một cách hợp lý.

CHÚ DẪN:

i_m phương tiện nối

I thiết bị nhập, ví dụ, cảm biến

L logic

m giám sát

O thiết bị xuất, ví dụ, công tắc tơ chính

TE thiết bị thử

OTE thiết bị xuất của TE

Hình 10 – Cấu trúc lựa chọn đối với loại 2

6.2.6 Loại 3

Đối với loại 3, phải áp dụng các yêu cầu tương tự như các yêu cầu theo 6.2.3 đối với loại B. Phải tuân theo các "nguyên tắc an toàn đã quen và đáng tin cậy" theo 6.2.4. Ngoài ra cần áp dụng yêu cầu sau.

Bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) loại 3 phải được thiết kế sao cho chỉ một lỗi trong bất cứ bộ phận nào cũng không dẫn đến việc mất đi chức năng an toàn. Bất cứ khi nào có thể thực hiện được thì lỗi tách biệt phải được phát hiện tại lúc hoặc trước khi có yêu cầu tiếp sau đối với chức năng an toàn.

Vùng chẩn đoán (DC_{avg}) của tổng SRP/CS bao gồm sự phát hiện lỗi phải thấp. $MTTF_d$ của mỗi một trong các kênh dư thừa phải là thấp – đến – cao tuỳ thuộc vào mức tính năng yêu cầu (PL_r). Phải áp dụng các biện pháp tránh lỗi do nguyên nhân chung (CCF) (xem Phụ lục F).

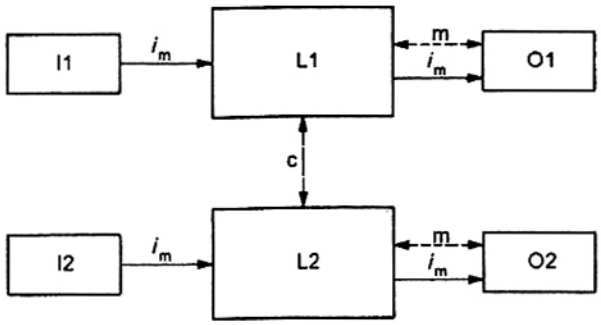
CHÚ THÍCH 1: Yêu cầu của việc phát hiện lỗi tách biệt không có nghĩa là tất cả các lỗi sẽ được phát hiện. Do đó, sự tích tụ các lỗi không được phát hiện có thể dẫn đến tín hiệu xuất không theo dự định và tình trạng khả thi để phát hiện lỗi là sử dụng liên hệ ngược (hồi tiếp) của các tiếp xúc rơ le được dẫn hướng cơ khí và giám sát công suất điện dư thừa.

CHÚ THÍCH 2: Nếu cần thiết, vì lý do công nghệ và ứng dụng, người biên soạn tiêu chuẩn loại C cần đưa ra thêm các nội dung chi tiết về việc phát hiện lỗi.

CHÚ THÍCH 3: Trạng thái của hệ thống loại 3 cho phép

- Khi xảy ra chỉ một lỗi, chức năng an toàn luôn được đảm bảo;
- Sẽ phát hiện được một số lỗi nhưng không phải tất cả các lỗi;
- Sự tích tụ của các lỗi không được phát hiện có thể dẫn đến việc làm mất đi chức năng an toàn.

CHÚ THÍCH 4: Công nghệ sử dụng ảnh hưởng đến khả năng thực hiện sự phát hiện ra lỗi.



Các đường nét đứt biểu thị sự phát hiện lỗi thực tế một cách hợp lý.

CHÚ DẪN:

i_m phương tiện nối

C giám sát chéo

I1, I2 thiết bị nhập, ví dụ, cảm biến

L1, L2 logic

m giám sát

O1, O2 thiết bị xuất, ví dụ, công tắc tơ chính

Hình 11 – Cấu trúc lựa chọn đối với loại 3

6.2.7 Loại 4

Đối với loại 4, phải áp dụng các yêu cầu tương tự như các yêu cầu theo 6.2.3 đối với loại B phải tuân theo các "nguyên tắc an toàn đã quen và đáng tin cậy" theo 6.2.4. Ngoài ra cần áp dụng yêu cầu sau.

Bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) loại 4 phải được thiết kế sao cho:

- Một lỗi tách biệt trong bất cứ bộ phận liên quan đến an toàn nào cũng không dẫn đến việc mất đi chức năng an toàn, và
- Lỗi tách biệt được phát hiện tại lúc hoặc trước khi có yêu cầu tiếp sau đối với chức năng an toàn, ví dụ, ngay khi đóng mạch hoặc lúc kết thúc chu trình vận hành của máy.

Nhưng nếu việc phát hiện này không thực hiện được thì sự tích tụ của các lỗi không được phát hiện không được dẫn đến việc làm mất đi chức năng an toàn.

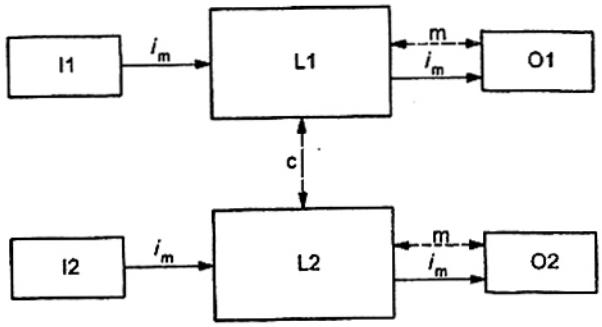
Vùng chẩn đoán (DC_{avg}) của tổng SRP/CS phải cao, bao gồm sự tích tụ của các lỗi. $MTTF_d$ của mỗi một trong các kênh dư thừa phải cao. Phải áp dụng các biện pháp tránh lỗi do nguyên nhân chung (CCF) (xem Phụ lục F).

CHÚ THÍCH 1: Trạng thái của hệ thống loại 4 cho phép.

- Khi xảy ra chỉ một lỗi, chức năng an toàn luôn được đảm bảo;
- Các lỗi sẽ được phát hiện kịp thời để ngăn ngừa sự mất đi chức năng an toàn;
- Tính đến sự tích tụ của các lỗi không được phát hiện.

CHÚ THÍCH 2: Sự khác nhau giữa loại 3 và loại 4 là DC_{avg} cao hơn trong loại 4 và $MTTF_d$ yêu cầu của mỗi kênh chỉ có "cao".

Trong thực tế, có thể phải xem xét đến một tổ hợp lỗi của hai lỗi.



Các đường nét liền cho giám sát biểu thị vùng chẩn đoán cao hơn trong cấu trúc lựa chọn đối với loại 3.

CHÚ DẪN:

i_m phương tiện nối
C giám sát ngang
I1, I2 thiết bị nhập, ví dụ, cảm biến
L1, L2 logic
m giám sát
O1, O2 thiết bị xuất, ví dụ, công tắc tơ chính

Hình 12 – Cấu trúc lựa chọn đối với loại 4

Bảng 10 – Tóm tắt các yêu cầu đối với các loại

Loại	Tóm tắt các yêu cầu	Trạng thái của hệ thống	Nguyên tắc sử dụng để đạt được an toàn	$MTTF_d$ của mỗi kênh	DC_{avg}	CCF
B (xem 6.2.3)	SRP/CS và/hoặc thiết bị bảo vệ cũng như các phần cấu thành của chúng phải được thiết kế, cấu trúc, lựa chọn, lắp ráp và phối hợp theo các tiêu chuẩn có liên quan để chúng chịu được ảnh hưởng yêu cầu. Phải sử dụng các nguyên tắc an toàn cơ bản	Sự xảy ra một lỗi có thể dẫn đến việc làm mất đi chức năng an toàn	Được đặc trưng chủ yếu bằng lựa chọn các bộ phận	Thấp đến trung bình	Không	Không có liên quan
1 (xem 6.2.4)	Phải áp dụng các yêu cầu của B. Phải sử dụng các bộ phận và nguyên tắc đã quen và đáng tin cậy	Sự xảy ra một lỗi có thể dẫn đến việc làm mất đi chức năng an toàn, nhưng xác suất xuất hiện thấp hơn đối với loại B	Được đặc trưng chủ yếu bằng lựa chọn các bộ phận	Cao	Không	Không có liên quan
2 (xem 6.2.5)	Phải áp dụng các yêu cầu của B. và sử dụng các nguyên tắc an toàn đã quen và đáng tin cậy. Phải kiểm tra chức năng an toàn ở các khoảng thời gian thích hợp bằng hệ thống kiểm tra của máy.	Sự xảy ra một lỗi có thể dẫn đến việc làm mất đi chức năng an toàn giữa các phép kiểm tra. Sự mất đi chức năng an toàn được phát hiện bằng kiểm tra	Được đặc trưng chủ yếu bằng cấu trúc	Thấp đến cao	Thấp đến trung bình	Xem Phụ lục F
3 (xem 6.2.5)	Phải áp dụng các yêu cầu của B và sử dụng các nguyên tắc an toàn đã quen và đáng tin cậy. Các bộ phận liên quan đến an toàn phải được thiết kế để – Một lỗi tách biệt trong bất cứ bộ phận nào cũng không dẫn đến việc làm mất đi chức năng an toàn, và – Bất cứ khi nào có thể thực hiện được thì lỗi tách biệt cần được phát hiện	Khi xảy ra một lỗi tách biệt thì chức năng an toàn luôn được đảm bảo	Được đặc trưng chủ yếu bằng cấu trúc	Thấp đến cao	Thấp đến trung bình	Xem Phụ lục F

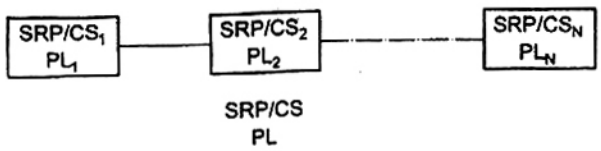
Bảng 10 – (kết thúc)

Loại	Tóm tắt các yêu cầu	Trạng thái của hệ thống	Nguyên tắc sử dụng để đạt được an toàn	$MTTF_d$ của mỗi kênh	DC_{avg}	CCF
4 (xem 6.2.7)	Phải áp dụng các yêu cầu của B và sử dụng các nguyên tắc an toàn đã quen và đáng tin cậy. Các bộ phận liên quan đến an toàn phải được thiết kế để – Một lỗi tách biệt trong bất cứ bộ phận nào cũng không dẫn đến việc làm mất đi chức năng an toàn, và – Lỗi tách biệt được phát hiện tại lúc hoặc trước khi có yêu cầu tiếp theo đối với chức năng an toàn, nhưng nếu sự phát hiện này không thể thực hiện được thì sự tích tụ các lỗi không được phát hiện không được dẫn đến việc làm mất đi chức năng an toàn	Khi xảy ra một lỗi tách biệt thì chức năng an toàn luôn được đảm bảo. Sựphát hiện ra các lỗi tích tụ làm giảm xác suất của sự mất đi chức năng an toàn (DC cao). Các lỗi sẽ được phát hiện kịp thời để ngăn ngừa sự mất đi của chức năng an toàn	Được đặc trưng chủ yếu bằng cấu trúc	Cao	Cao bao gồm sự tích tụ các lỗi	Xem Phụ lục F
CHÚ THÍCH: Đối với các yêu cầu đầy đủ, xem Điều 6.						

6.3 Tổ hợp của các SRP/CS để đạt được mức tính năng (PL) toàn bộ

Một chức năng an toàn có thể được thực hiện bởi một tổ hợp nhiều bộ phận liên quan đến an toàn (SRP/CS): hệ thống nhập, thiết bị xử lý tín hiệu, hệ thống xuất. Các SRP/CS này có thể được gán cho một và/hoặc các loại khác nhau. Đối với mỗi SRP/CS được sử dụng, phải lựa chọn một loại theo 6.2. Đối với tổ hợp chung của các SRP/CS này, có thể xác định PL toàn bộ bằng Bảng 11. Trong trường hợp này cần có sự phê duyệt tổ hợp của các SRP/CS (xem Hình 3).

Theo 6.2, các bộ phận liên quan đến an toàn được tổ hợp lại của một hệ thống điều khiển khởi động ở các điểm tại đó các tín hiệu liên quan đến an toàn được bắt đầu và kết thúc tại đầu ra của các phần tử điều khiển công suất. Nhưng các SRP/CS được tổ hợp có thể bao gồm nhiều bộ phận được nối theo một đường thẳng (xếp hàng nối tiếp) hoặc theo cách dư thừa (xếp hàng song song). Để tránh sự dự đoán phức tạp mới đối với mức tính năng (PL) đạt được bởi các SRP/CS được tổ hợp ở đó các PL riêng biệt đã được tính toán sẵn, cần thực hiện các dự tính sau cho sự xếp hàng nối tiếp của SRP/CS. Giả thử N là các SRP/CS_i riêng biệt trong sự xếp hàng nối tiếp và được xem như một tổ hợp tạo thành một chức năng an toàn. Đối với mỗi SRP/CS_i, một PL_i đã được ước lượng. Tình trạng này được minh hoạ trên Hình 13 (xem Hình 4 và Hình 2).



Hình 13 – Tổ hợp của SRP/CS để đạt được PL toàn bộ

Phương pháp sau cho phép tính toán PL của toàn bộ các SRP/CS đã được tổ hợp để tạo thành chức năng an toàn:

a) Nhận biết PL_i thấp nhất: đó là PL_{low}.

b) Nhận biết số $N_{low} \leq N$ của SRP/CS_i, với $PL_i = PL_{low}$.

c) Tra PL trong Bảng 11.

Bảng 11 – Tính toán PL đối với sự chỉnh hàng nối tiếp của các SRP/CS

PL_{low}	N_{low}	=>	PL
a	> 3	=>	Không, không cho phép
	≤ 3	=>	a
b	> 2	=>	a
	≤ 2	=>	b
c	> 2	=>	b
	≤ 2	=>	c
d	> 3	=>	c
	≤ 3	=>	d
e	> 3	=>	d
	≤ 3	=>	e

CHÚ THÍCH: Các giá trị được tính toán cho việc tra bảng này dựa trên các giá trị độ tin cậy tại điểm giữa của mỗi PL.

7 Xem xét lỗi, ngăn chặn lỗi

7.1 Quy định chung

Theo loại được lựa chọn, phải thiết kế các bộ phận liên quan đến an toàn để đạt được mức tính năng yêu cầu (PL_r). Khả năng tránh được lỗi phải được đánh giá.

7.2 Xem xét lỗi

TCVN 7384-2 (ISO 13849-2) liệt kê các lỗi quan trọng và hư hỏng đối với các công nghệ khác nhau. Bản kê của các lỗi là không thể thiếu được và nếu cần, phải xem xét và liệt kê các lỗi bổ sung. Trong những trường hợp này, phương pháp ước lượng cũng nên được thảo luận rõ ràng. Đối với các bộ phận mới không được nêu trong TCVN 7384-2 (ISO 13849-2), phải thực hiện một dạng hư hỏng và phân tích các ảnh hưởng (FMEA, xem IEC 60812) để xác lập các lỗi cần được xem xét đối với các bộ phận này.

Thông thường, phải tính đến các chuẩn cứ sau của lỗi:

- Nếu do hậu quả của một lỗi, các bộ phận sẽ hư hỏng thêm thì lỗi đầu tiên cùng tất cả các lỗi theo sau phải được xem là chỉ một lỗi (lỗi đơn);
- Hai hoặc nhiều lỗi tách biệt có một nguyên nhân chung phải được xem như chỉ một lỗi (lỗi đơn) (như đã biết là CCF);
- Sự xảy ra đồng thời của hai hoặc nhiều lỗi có các nguyên nhân riêng biệt được xem là rất có thể không chắc đã đúng và do đó không cần phải xem xét.

7.3 Ngăn chặn lỗi

Thông thường không có thể ước lượng các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) mà không giả thiết rằng có thể ngăn chặn một số lỗi. Để có thông tin chi tiết hơn về sự ngăn chặn lỗi, xem TCVN 7384-2 (ISO 13849-2).

Ngăn chặn lỗi là một sự thoả hiệp giữa các yêu cầu kỹ thuật an toàn và khả năng lý thuyết xảy ra một lỗi.

Sự ngăn chặn lỗi có thể dựa trên:

- Sự không chắc xảy ra về mặt kỹ thuật đối với một số lỗi;
- Kinh nghiệm về mặt kỹ thuật thường được chấp nhận, không phụ thuộc vào ứng dụng được xem xét, và
- Các yêu cầu kỹ thuật có liên quan đến ứng dụng và mối nguy hiểm riêng.

Nếu các lỗi được ngăn chặn thì phải đưa ra sự biện luận tỷ mỷ trong tài liệu kỹ thuật.

8 Phê duyệt

Thiết kế của bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) phải được phê duyệt (xem Hình 3). Việc phê duyệt phải chứng minh rằng tổ hợp của các SRP/CS cung cấp mỗi chức năng an toàn đáp ứng được tất cả các yêu cầu có liên quan đến tiêu chuẩn này.

Đối với các nội dung chi tiết của phê duyệt, xem TCVN 7384-2 (ISO 13849-2).

9 Bảo dưỡng

Có thể cần phải bảo dưỡng dự phòng hoặc bảo dưỡng sửa chữa để duy trì tính năng làm việc quy định của các bộ phận liên quan đến an toàn. Các sai lệch về thời gian so với tính năng làm việc quy định có thể dẫn đến sự suy giảm về an toàn hoặc thậm chí dẫn đến tình trạng nguy hiểm. Thông tin cho sử dụng của SRP/CS phải bao gồm các hướng dẫn về bảo dưỡng (bao gồm cả kiểm tra định kỳ) của các SRP/CS.

Các quy định về bảo dưỡng các bộ phận liên quan đến an toàn của một hệ thống điều khiển phải tuân theo các nguyên tắc cho trong 4.7, TCVN 7383-2. Tất cả các thông tin về bảo dưỡng phải tuân theo TCVN 7383-2, trong 6.5.1 e).

10 Cung cấp tài liệu kỹ thuật

Khi thiết kế một bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS), người thiết kế phải cung cấp tư liệu ít nhất là về các thông tin sau đối với bộ phận liên quan đến an toàn:

- Chức năng an toàn do SRP/CS cung cấp;
- Đặc tính của mỗi chức năng an toàn;
- Các điểm chính xác tại đó bộ phận liên quan đến an toàn bắt đầu (khởi động) và kết thúc;
- Điều kiện môi trường;
- Mức tính năng (PL);
- Loại hoặc các loại được lựa chọn;
- Các tham số liên quan đến độ tin cậy ($MTTF_d$, DC, CCF và thời gian làm việc);
- Các biện pháp tránh các hư hỏng có hệ thống;
- Công nghệ hoặc các công nghệ được sử dụng;
- Tất cả các lỗi liên quan đến an toàn được xem xét;
- Biện luận hoặc giải thích về sự ngăn chặn lỗi [xem TCVN 7384-2 (ISO 13849-2)];
- Lý do cơ bản của thiết kế (ví dụ, các lỗi được xem xét, các lỗi được ngăn chặn);

- Tài liệu phần mềm;
- Các biện pháp chống sử dụng sai hợp lý thấy trước.

CHÚ THÍCH: Thông thường việc cung cấp các tài liệu này được xem là mục đích nội tại của nhà sản xuất và sẽ không được phân cho người sử dụng máy.

11 Thông tin cho sử dụng

Phải áp dụng các nguyên tắc của TCVN 7383-2:2004 (ISO 12100-2:2003), trong 6.5.2 và các phần áp dụng được của các tài liệu có liên quan (ví dụ, IEC 60204-1:2005, Điều 17). Đặc biệt là phải cung cấp cho người sử dụng thông tin quan trọng về sử dụng an toàn các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS). Thông tin này ít nhất phải bao gồm:

- Các giới hạn của các bộ phận liên quan đến an toàn cho các loại được lựa chọn và bất cứ sự ngăn chặn lỗi nào;
- Các giới hạn của các SRP/CS và bất cứ sự ngăn chặn lỗi nào (xem 7.3), khi được dùng chủ yếu để duy trì loại hoặc các loại đã lựa chọn và đặc tính an toàn thì phải đưa ra thông tin thích hợp (ví dụ, để cải tiến, bảo dưỡng và sửa chữa) để bảo đảm sự biện minh cho việc ngăn chặn lỗi;
- Các ảnh hưởng của sai lệch so với tính năng làm việc quy định về chức năng an toàn;
- Mô tả rõ ràng các giao diện của SRP/CS và thiết bị bảo vệ;
- Thời gian đáp ứng;
- Các giới hạn cho hoạt động (bao gồm cả điều kiện môi trường);
- Các chỉ báo và báo động (cảnh báo);
- Sự tạm ngừng và đình chỉ các chức năng an toàn;
- Các chế độ điều khiển;
- Bảo dưỡng (xem Điều 9);
- Bản kê kiểm tra bảo dưỡng;
- Dễ dàng tiếp cận và thay thế các chi tiết bên trong;
- Các biện pháp khắc phục (xử lý) trục trặc dễ dàng và an toàn;
- Thông tin giải thích các ứng dụng cho sử dụng liên quan đến loại được viện dẫn;
- Các khoảng thời gian thử nghiệm kiểm tra có liên quan.

Phải cung cấp thông tin riêng về loại hoặc các loại và mức tính năng (PL) của các SRP/CS như sau:

- Tham chiếu tiêu chuẩn này của TCVN 7384 (ISO 13849), [ví dụ "TCVN 7384-1:2010 (ISO 13849-1:2006)"];
- Loại, B,1,2,3 hoặc 4;
- Mức tính năng, a, b, c, d, hoặc e.

VÍ DỤ: Một SRP/CS theo phiên bản này của TCVN 7384-1 (ISO 13849-1), loại B và mức tính năng a có thể được viện dẫn như sau:

TCVN 7384-1:2010 (ISO 13849-1:2006) , Loại B PL a.

Phụ lục A

(Tham khảo)

Xác định mức tính năng yêu cầu (PL_r)

A.1 Lựa chọn PL_r

Phụ lục này đề cập đến sự đóng góp vào việc giảm rủi ro được thực hiện bởi các bộ phận liên quan đến an toàn của hệ thống điều khiển đang được xem xét. Phương pháp đưa ra ở đây chỉ cung cấp sự dự tính về giảm rủi ro và được dùng như hướng dẫn cho người thiết kế và người biên soạn tiêu chuẩn trong việc xác định PL_r đối với mỗi chức năng an toàn cần thiết do bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) thực hiện.

Việc đánh giá rủi ro thừa nhận một tình trạng trước khi cung cấp chức năng an toàn dự định sử dụng. Có thể tính đến việc giảm rủi ro bằng các biện pháp kỹ thuật khác không phụ thuộc vào hệ thống điều khiển (ví dụ, các bộ phận bảo vệ cơ khí), hoặc các chức năng an toàn bổ sung khi xác định PL_r của chức năng an toàn dự định sử dụng, trong trường hợp như vậy, có thể chọn điểm bắt đầu của Hình A.1 sau khi thực hiện các biện pháp này (xem Hình 2). Tính nghiêm trọng của thương tích (được biểu thị bởi S) sẽ khá dễ dàng cho dự tính (ví dụ, sự xé rách, sự cắt cụt, chết người). Đối với tần suất xảy ra thương tích, sử dụng các tham số phụ để cải thiện sự dự tính. Các tham số này là:

– Tần suất và thời gian phơi ra trước mối nguy hiểm (F), và

– Khả năng tránh nguy hiểm hoặc hạn chế tổn hại (P).

Kinh nghiệm chỉ ra rằng các tham số này có thể được kết hợp lại, như trên Hình A.1, để đưa ra sự phân cấp rủi ro từ thấp đến cao. Cần nhấn mạnh rằng đây là một quá trình định tính chỉ đưa ra sự dự tính rủi ro.

A.2 Hướng dẫn lựa chọn các tham số S, F và P cho dự tính rủi ro

A.2.1 Tính nghiêm trọng của thương tích S1 và S2

Trong việc dự tính rủi ro xuất hiện từ một hư hỏng của một chức năng an toàn thì chỉ quan tâm đến các thương tích nhẹ (thường có thể chữa khỏi được) và các thương tích nghiêm trọng (thường không thể chữa khỏi được) và chết người.

Để có quyết định, nên tính đến hậu quả của các vụ tai nạn và các quá trình chữa lành thương tích thông thường khi xác định S1 và S2. Ví dụ, gây ra các vết thâm tím, vết rách không có các biến chứng có thể được xếp vào loại S1, trong khi sự cắt cụt hoặc chết người được xếp vào loại S2.

A.2.2 Tần suất và/ hoặc thời gian phơi ra trước nguy hiểm, F1 và F2

Thông thường có thể không quy định khoảng thời gian có hiệu lực được lựa chọn cho tham số F1 hoặc F2. Tuy nhiên, sự giải thích sau đây có thể tạo điều kiện dễ dàng cho việc đưa ra quyết định đúng khi còn có sự nghi ngờ.

Nên lựa chọn F2 nếu một người thường xuyên hoặc liên tục bị phơi ra trước mối nguy hiểm. Sẽ là không thích hợp khi cùng một người hoặc nhiều người khác nhau bị phơi ra trước mối nguy hiểm với thời gian phơi liên tục, ví dụ như để sử dụng thang máy. Tham số tần suất nên được lựa chọn theo tần số và khoảng thời gian tiếp cận với mối nguy hiểm.

Khi người thiết kế biết được yêu cầu đối với chức năng an toàn thì tần suất và khoảng thời gian của yêu cầu này có thể được lựa chọn thay cho tần suất và khoảng thời gian tiếp cận với mối nguy hiểm. Trong tiêu chuẩn này, tần suất của yêu cầu đối với chức năng an toàn được giả thiết là lớn hơn một lần trên năm.

Khoảng thời gian phơi ra trước mối nguy hiểm nên được ước lượng dựa trên cơ sở một giá trị trung bình được biết là có liên quan đến tổng thời gian sử dụng thiết bị. Ví dụ, nếu cần thiết phải đi tới một cách đều đặn giữa các dụng cụ của máy trong quá trình làm việc có chu kỳ để dẫn tiến và di chuyển chi tiết gia công thì nên lựa chọn F2. Nếu sự tiếp cận chỉ thỉnh thoảng mới yêu cầu thì nên lựa chọn F1.

CHÚ THÍCH: Trong trường hợp không có sự biện minh nào khác thì nên lựa chọn F2, nếu tần suất cao hơn một lần trên giờ.

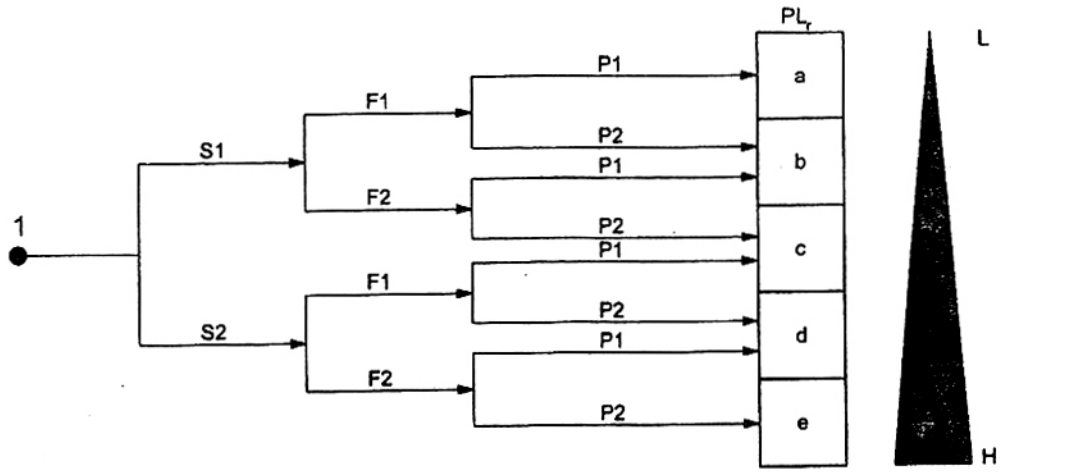
A.2.3 Khả năng tránh mối nguy hiểm P1 và P2

Điều quan trọng là phải biết một tình trạng nguy hiểm có thể được nhận ra và tránh được hay không trước khi dẫn đến một tai nạn. Ví dụ, sự xem xét quan trọng là mối nguy hiểm có thể nhận biết được một cách trực tiếp hay không bởi đặc tính vật lý của nó hoặc chỉ được nhận ra bởi các phương tiện kỹ thuật, ví dụ, các bộ phận chỉ báo. Các khía cạnh quan trọng khác ảnh hưởng tới việc lựa chọn tham số P bao gồm, ví dụ:

- Vận hành có hoặc không có sự giám sát;
- Vận hành bởi chuyên gia hoặc người không lành nghề;
- Tốc độ tại đó nảy sinh mối nguy hiểm (ví dụ, nhanh hoặc chậm);
- Các khả năng tránh nguy hiểm (ví dụ, bằng thoát hiểm);
- Các kinh nghiệm thực tế về an toàn liên quan đến quá trình.

Khi xảy ra một tình trạng nguy hiểm, chỉ nên lựa chọn P1 nếu có cơ hội thực sự tránh được vụ tai nạn hoặc giảm một cách đáng kể ảnh hưởng của nó, nên chọn P2 nếu hầu như không có cơ hội tránh được mối nguy hiểm.

Hình A.1 đưa ra hướng dẫn để xác định PL_r liên quan đến an toàn phụ thuộc vào sự đánh giá rủi ro. Biểu đồ cần được xem xét cho chức năng an toàn. Phương pháp đánh giá rủi ro được dựa trên TCVN 7301 (ISO 14121) và nên được sử dụng theo TCVN 7383-1 (ISO 12100-1).



CHÚ DẪN	CÁC THAM SỐ RỦI RO
1 Điểm bắt đầu cho ước lượng sự đóng góp của chức năng an toàn vào giảm rủi ro	S Tính nghiêm trọng của thương tích nhẹ (thương tích S1 thường chữa khỏi được)
L Sự đóng góp thấp vào giảm rủi ro	S2 Nghiêm trọng (thương tích thường không chữa khỏi được hoặc chết người)
H Sự đóng góp cao vào giảm rủi ro	F Tần suất và / hoặc sự phơi ra trước mối nguy hiểm
PL_r Mức tính năng yêu cầu	F1 Thời gian phơi ít khi - đến - ít - thường xuyên và / hoặc thời gian phơi ngắn
	F2 Thời gian phơi thường xuyên - đến - liên tục và / hoặc thời gian phơi dài
	P Khả năng tránh nguy hiểm hoặc hạn chế tổn hại
	P1 Có thể trong điều kiện quy định
	P2 Chắc là không thể

Hình A.1 - Biểu đồ rủi ro để xác định PL_r đối với chức năng an toàn

Phụ lục B

(Tham khảo)

Phương pháp lập sơ đồ khối và sơ đồ khối liên quan đến an toàn

B.1 Phương pháp lập sơ đồ khối

Phương pháp đơn giản hoá đòi hỏi sự biểu thị các khối liên kết với nhau theo hướng logic của các bộ phận liên qua đến an toàn của hệ thống điều khiển (SRP/CS). SRP/CS nên được tách ly thành một số lượng nhỏ các khối theo yêu cầu sau:

- Các khối nên biểu thị bộ logic của SRP/CS liên quan đến việc thực hiện chức năng an toàn;
- Các kênh khác nhau thực hiện chức năng an toàn nên được tách ly thành các khối khác nhau - nếu một khối không còn khả năng thực hiện chức năng an toàn của nó thì việc thực hiện chức năng an toàn qua các khối của các kênh khác sẽ không bị ảnh hưởng;
- Mỗi kênh có thể gồm có một hoặc nhiều khối – ba khối trong một kênh trong các cấu trúc đã lựa chọn, khối nhập, khối logic và khối xuất không phải là số lượng bắt buộc, nhưng đơn giản chỉ là một ví dụ đối với sự chia tách bên trong mỗi kênh;
- Mỗi đơn vị phần cứng của SRP/CS nên thuộc vào một khối, như vậy cho phép tính toán $MTTF_d$ của khối dựa trên $MTTF_d$ của các đơn vị phần cứng thuộc vào khối (ví dụ, bằng dạng hư hỏng và phân tích các ảnh hưởng hoặc phương pháp đếm các bộ phận, xem Phụ lục D.1);
- Các đơn vị phần cứng chỉ được sử dụng để chẩn đoán (ví dụ, thiết bị thử) và không ảnh hưởng đến việc thực hiện chức năng an toàn trong các kênh khác nhau khi chúng hư hỏng một cách nguy hiểm, chúng có thể được tách ra khỏi các đơn vị phần cứng cần thiết để thực hiện chức năng an toàn trong các kênh khác nhau.

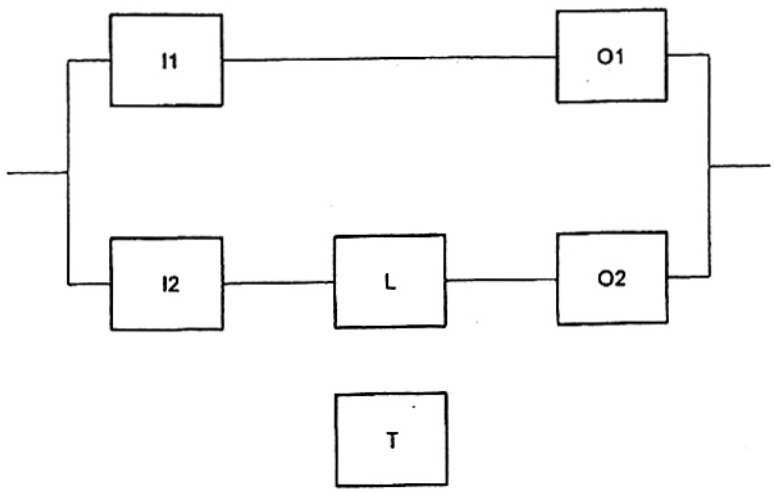
CHÚ THÍCH: Đối với phần mềm này của TCVN 7384-1 (ISO 13849-1), "các khối" không tương đương với các khối chức năng hoặc các khối độ tin cậy.

B.2 Sơ đồ khối liên quan đến an toàn

Các khối được xác định bằng phương pháp lập sơ đồ khối có thể được dùng để biểu thị bằng hình vẽ cấu trúc logic của SRP/CS trong một sơ đồ khối liên quan đến an toàn. Đối với cách biểu thị bằng hình vẽ này cần theo hướng dẫn sau:

- Hư hỏng của một khối trong sự xếp hàng nối tiếp các khối dẫn tới hư hỏng của toàn bộ kênh (ví dụ, nếu một đơn vị phần cứng trong một kênh của SRP/CS hư hỏng một cách nguy hiểm thì toàn bộ kênh không thể có khả năng thực hiện chức năng an toàn được nữa);
- Chỉ có hư hỏng nguy hiểm của tất cả các kênh trong sự xếp hàng song song mới dẫn đến sự mất đi chức năng an toàn (ví dụ, một chức năng an toàn tạo thành bởi nhiều kênh chỉ được thực hiện với điều kiện là ít nhất phải có một kênh không bị hư hỏng);
- Các khối chỉ dùng cho mục đích thử nghiệm và không ảnh hưởng đến chức năng an toàn trong các kênh khác nhau, khi chúng hư hỏng một cách nguy hiểm có thể được tách ra khỏi các khối trong các kênh khác nhau.

Xem ví dụ Hình B.1



I1 và O1 lắp trên kênh thứ nhất (xếp hàng nối tiếp); trong khi I2, L và O2 lắp trên kênh thứ hai (xếp hàng nối tiếp), với cả hai kênh thực hiện chức năng an toàn dư thừa (xếp hàng song song). T chỉ được sử dụng cho thử nghiệm.

CHÚ DẪN

I1, I2 các thiết bị nhập, ví dụ, cảm biến

L logic

O1, O2 các thiết bị xuất, ví dụ công tắc tơ chính

T thiết bị thử

Hình B.1 – Ví dụ về sơ đồ khối liên quan đến an toàn

Phụ lục C
(Tham khảo)

Tính toán hoặc ước lượng các giá trị $MTTF_d$ cho các bộ phận đơn

C.1 Quy định chung

Phụ lục này đưa ra nhiều phương pháp để tính toán hoặc ước lượng các giá trị $MTTF_d$ cho các bộ phận đơn: phương pháp được nêu trong C.2 dựa trên quy trình kỹ thuật tốt đối với các loại bộ phận khác nhau; phương pháp được nêu trong C.3 áp dụng cho các bộ phận thuỷ lực; C.4 đưa ra phương thức tính toán $MTTF_d$ của các bộ phận khí nén, cơ khí và điện - cơ từ B_{10} (xem C.4.1); C.5 liệt kê các giá trị $MTTF_d$ cho các bộ phận điện.

C.2 Phương pháp quy trình kỹ thuật tốt

Nếu đáp ứng các chuẩn sau, MTTFd hoặc giá trị B_{10d} đối với một bộ phận có thể được dự tính theo Bảng C.1.

a) Các bộ phận được chế tạo theo các nguyên tắc cơ bản và đã quen - đáng tin cậy phù hợp với TCVN 7384-2:2010 (ISO 13849-2:2003), hoặc tiêu chuẩn có liên quan (xem Bảng C.1) để thiết kế bộ phận (sự chứng thực trong tờ dữ liệu của bộ phận).

CHÚ THÍCH: Có thể tìm thấy thông tin này trong bảng dữ liệu của nhà sản xuất bộ phận.

b) Nhà sản xuất bộ phận quy định việc ứng dụng thích hợp và các điều kiện làm việc cho người sử dụng.

c) Việc thiết kế các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) đáp ứng các nguyên tắc cơ bản và đã quen – đáng tin cậy phù hợp với TCVN 7384-2:2010 (ISO 13849-2:2003) để thực hiện và vận hành bộ phận.

C.3 Bộ phận thuỷ lực

Nếu đáp ứng các tiêu chuẩn sau, giá trị $MTTF_d$ đối với một bộ phận thủy lực đơn, ví dụ, van, có thể được dự tính là 150 năm.

a) Các bộ phận thuỷ lực được chế tạo theo các nguyên tắc cơ bản và đã quen – đáng tin cậy phù hợp với TCVN 7384-2:2010 (ISO 13849-2:2003), Bảng C.1 và Bảng C.2 để thiết kế bộ phận thuỷ lực (sự chứng thực trong tờ dữ liệu của bộ phận).

CHÚ THÍCH: Có thể tìm thấy thông tin này trong bảng dữ liệu của nhà sản xuất bộ phận.

b) Nhà sản xuất bộ phận quy định việc ứng dụng thích hợp và các điều kiện làm việc cho người sử dụng. Nhà sản xuất SRP/CS phải cung cấp thông tin gắn liền với trách nhiệm của mình để áp dụng các nguyên tắc cơ bản và đã quen – đáng tin cậy phù hợp với TCVN 7384-2:2010 (ISO 13849-2:2003), Bảng C.1 và C.2 để thực hiện và vận hành bộ phận thuỷ lực.

Nhưng nếu a) hoặc b) không đạt được thì nhà sản xuất phải đưa ra giá trị $MTTF_d$ đối với bộ phận thuỷ lực đơn.

Bảng C.1 – Các tiêu chuẩn quốc tế về $MTTF_d$ hoặc B_{10d} đối với các bộ phận

	Các nguyên tắc cơ bản và đã quen - đáng tin cậy theo TCVN 7384-2:2010 (ISO 13849-2:2003)	Các tiêu chuẩn có liên quan khác	Các giá trị điển hình: $MTTF_d$ (năm) B_{10d} (chu kỳ)
Bộ phận cơ khí	Các Bảng A.1 và A.2	–	$MTTF_d$ = 150
Bộ phận thuỷ lực	Các Bảng C.1 và C.2	EN 982	$MTTF_d$ = 150
B ộ phận khí nén	Các Bảng B.1 và B.2	EN 983	B_{10d} = 20 000 000
Rơle và công tắc tơ - rơle có tải trọng nhỏ (tải trọng cơ khí)	Các Bảng D.1 và D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20 000 000
Rơle và công tắc tơ - rơle có tải trọng lớn	Các Bảng D.1 và D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400 000
Công tắc ở gần có tải trọng nhỏ (tải trọng cơ khí)	Các Bảng D.1 và D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Công tắc ở gần có tải trọng lớn	Các Bảng D.1 và D.2	IEC 60947 EN 1088	B_{10d} = 4 000 000
Công tắc tơ có tải trọng nhỏ (tải trọng cơ khí)	Các Bảng D.1 và D.2	IEC 60947	B_{10d} = 20 000 000
Công tắc tơ có tải trọng danh định	Các Bảng D.1 và D.2	IEC 60947	B_{10d} = 2 000 000
Công tắc vị trí không phụ thuộc vào tải [a]	Các Bảng D.1 và D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Công tắc vị trí (có cơ cấu tác động riêng, khoá hãm - bảo vệ) không phụ thuộc vào tải trọng [a]	Các Bảng D.1 và D.2	IEC 60947 EN 1088	B_{10d} = 2 000 000
Cơ cấu dừng khẩn cấp không phụ thuộc vào tải trọng [a]	Các Bảng D.1 và D.2	IEC 60947 ISO 13850	B_{10d} = 100 000
Cơ cấu dừng khẩn cấp có yêu cầu làm việc tối đa	Các Bảng D.1 và D.2	IEC 60947 TCVN 6719 (ISO 13850)	B_{10d} = 6 050
Nút ấn (ví dụ, công tắc thích nghi) không phụ thuộc vào tải trọng [a]	Các Bảng D.1 và D.2	IEC 60947	B10d = 100 000
Xem định nghĩa và sử dụng B_{10d} trong C.4. CHÚ THÍCH 1 – B_{10d} được dự tính là hai lần B_{10} (50 % hư hỏng nguy hiểm). CHÚ THÍCH 2 – "tải trọng nhỏ" có nghĩa là 20 % giá trị danh định (để có thêm thông tin, xem EN 13849-2)			
[a] Có thể mở trực tiếp nếu ngăn chặn được lỗi.			

C.4 $MTTF_d$ của các bộ phận khí nén, cơ khí và điện-cơ

C.4.1 Quy định chung

Đối với các bộ phận khí nén, cơ khí và điện cơ (van khí nén, rơle, công tắc tơ, công tắc vị trí, cam của công tắc vị trí, v.v...) có thể có khó khăn trong tính toán thời gian trung bình tới khi hư hỏng nguy hiểm ($MTTF_d$ cho các bộ phận), được tính bằng năm và theo yêu cầu của tiêu chuẩn này. Phần lớn thời gian, các nhà sản xuất các loại bộ phận này chỉ đưa ra số trung bình các chu kỳ tới 10 % các bộ phận bị hư hỏng nguy hiểm (B_{10d}). Điều này đưa ra phương pháp tính toán $MTTF_d$ cho các bộ phận bằng cách sử dụng B_{10} hoặc T (tuổi thọ) do nhà sản xuất cung cấp có liên quan chặt chẽ với số chu kỳ phụ thuộc vào ứng dụng.

Giá trị $MTTF_d$ đối với một bộ phận khí nén, điện cơ hoặc cơ khí đơn có thể được dự tính theo C.4.2 nếu đáp ứng các chuẩn sau

a) Các bộ phận được chế tạo theo các nguyên tắc an toàn cơ bản phù hợp với TCVN 7384-2:2004 (ISO 13849-2:2003), Bảng D.1 để thiết kế bộ phận (sự chứng thực trong tờ dữ liệu của bộ phận).

CHÚ THÍCH: Có thể tìm thấy thông tin này trong bảng dữ liệu của nhà sản xuất bộ phận.

b) Các bộ phận sử dụng trong loại 1, 2, 3 hoặc 4 được chế tạo theo các nguyên tắc an toàn đã quen - đáng tin cậy phù hợp với TCVN 7384-2:2004 (ISO 13849-2:2003), Bảng B.2 hoặc D.2 để thiết kế bộ phận (sự chứng thực trong tờ dữ liệu của bộ phận).

CHÚ THÍCH: Có thể tìm thấy thông tin này trong tờ dữ liệu của nhà sản xuất bộ phận.

c) Nhà sản xuất bộ phận quy định việc ứng dụng thích hợp và các điều kiện làm việc cho người sử dụng. Nhà sản xuất SRP/CS phải cung cấp thông tin gắn liền với trách nhiệm của mình để đáp ứng các nguyên tắc an toàn cơ bản phù hợp với TCVN 7384-2:2004 (ISO 13849-2:2003), Bảng B.1 hoặc D.1 để thực hiện và vận hành bộ phận. Đối với loại 1, 2, 3 hoặc 4, người sử dụng phải được thông báo về trách nhiệm của mình trong việc thực hiện các nguyên tắc an toàn đã quen - đáng tin cậy phù hợp với TCVN 7384-2:2004 (ISO 13849-2:2003), Bảng B.2 hoặc D.2 để thực hiện và vận hành bộ phận.

C.4.2 Tính toán $MTTF_d$ cho các bộ phận từ B_{10d}

Số các chu kỳ trung bình tới 10 % các bộ phận bị hư hỏng nguy hiểm (B_{10d})[3] cần được xác định bởi nhà sản xuất bộ phận theo các tiêu chuẩn sản phẩm có liên quan dùng cho các phương pháp thử nghiệm (ví dụ, IEC 60957-5-1, ISO 19973, IEC 61810). Các dạng hư hỏng nguy hiểm của các bộ phận phải được định nghĩa, ví dụ, sự kẹt ở vị trí cuối, hoặc sự thay đổi của các thời gian chuyển mạch. Nếu không phải tất cả các bộ phận bị hư hỏng trong quá trình thử nghiệm (ví dụ, bảy bộ phận được thử nghiệm chỉ có năm bị hư hỏng nguy hiểm) thì cần tính đến sự phân tích các bộ phận không bị hư hỏng

[3] Nếu không cho phần nguy hiểm của B_{10} thì có thể sử dụng 50 % của B_{10}, nên lấy $B_{10d} = 2\ B_{10}$.

nguy hiểm. Với $_{B10}$ và n_{op}, số lượng trung bình của các hoạt động hàng năm thì có thể tính toán $MTTF_d$ cho các bộ phận như sau

$$\mathrm{MTTF_d} = \frac{B_{10d}}{0,1 \times \mathrm{n_{op}}} \quad \text{(C.1)}$$

trong đó

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600\, s/h}{t_{cycle}} \quad \text{(C.2)}$$

với giả thiết đã được đặt ra cho ứng dụng của bộ phận:

h_{op} là hoạt động trung bình, tính bằng giờ trên ngày;

d_{op} là hoạt động trung bình, tính bằng ngày trên năm;

t_{cycle} là thời gian trung bình giữa sự bắt đầu của hai chu kỳ liên tiếp của bộ phận (ví dụ, chuyển mạch van), tính bằng giây trên chu kỳ.

Thời gian hoạt động của bộ phận được giới hạn tới T_{10d}, thời gian trung bình tới khi 10 % các bộ phận bị hư hỏng nguy hiểm:

$$T_{10d} = \frac{B_{10d}}{n_{op}} \quad \text{(C.3)}$$

CHÚ THÍCH: Công thức được giải thích trong C.4.2

B_{10d}, số lượng trung bình của các chu kỳ tới khi 10 % các bộ phận bị hư hỏng nguy hiểm, có thể được chuyển đổi thành T_{10d}, thời gian trung bình tới khi 10 % các bộ phận bị hư hỏng nguy hiểm, bằng cách sử dụng n_{op}, số lượng trung bình của các hoạt động hàng năm

$$T_{10d} = \frac{B_{10d}}{n_{op}} \quad \text{(C.4)}$$

Các phương pháp tin cậy trong tiêu chuẩn này thừa nhận rằng các bộ phận hư hỏng của các bộ phận được phân bố theo hàm số mũ đối với thời gian: $F(t) = 1 - \exp(-\lambda d t)$. Đối với các bộ phận khí nén và điện - cơ thì sự phân bố có thể là phân bố Weibull. Nhưng nếu thời gian hoạt động của các bộ phận được giới hạn đến thời gian trung bình tới khi 10 % các bộ phận bị hư hỏng nguy hiểm (T_{10d}), thì tần suất hư hỏng nguy hiểm không đổi (λd) trong thời gian hoạt động này có thể được dự tính là

$$\lambda d \approx \frac{0,1}{T_{10d}} = \frac{0,1 \times n_{op}}{B_{10d}} \quad \text{(C.5)}$$

Phương trình (C.5) có tính đến trường hợp với một tần suất hư hỏng không đổi, 10 % các bộ phận trong ứng dụng được giả thiết là bị hư hỏng sau T_{10d} (tính bằng năm) tương đương với B_{10d} (tính bằng chu kỳ). Chính xác hơn là:

$$F(T_{10d}) = 1 - \exp(-\lambda d T_{10d}) = 10\ \%\ \text{nghĩa là}\ \lambda d \approx -\frac{\ln(0,9)}{T_{10d}} = \frac{0,10536}{T_{10d}} \approx \frac{0,1}{T_{10d}} \quad (C.6)$$

Với $MTTF_d = 1/\lambda d$ đối với các phân bố theo hàm số mũ, phương trình dẫn đến

$$MTTF_d = \frac{T_{10d}}{0,1} = \frac{B_{10d}}{0,1 \times n_{op}} \quad (C.7)$$

C.4.3 Ví dụ

Đối với một van khí nén, nhà sản xuất xác định một giá trị trung bình 60 triệu chu kỳ là B_{10d}. Van được sử dụng cho hai ca mỗi ngày với 220 ngày làm việc một năm. Thời gian trung bình giữa lúc bắt đầu của hai lần chuyển mạch liên tiếp của van được dự tính là 5 s. Do đó có các giá trị sau:

- d_{op} là 220 ngày trên năm;
- h_{op} là 16 h trên ngày;
- t_{cycle} là 5 s trên chu kỳ;
- B_{10d} là 60 triệu chu kỳ.

Với các dữ liệu nhập này có thể tính toán các đại lượng sau:

$$n_{op} = \frac{220\ \text{ngày/năm} \times 16\ \text{h/ngày} \times 3600\ \text{s/h}}{5\ \text{s/chu kỳ}} = 2,53 \times 10^6\ \text{chu kỳ/năm} \quad (C.8)$$

$$T_{10d} = \frac{60 \times 10^6\ \text{năm}}{2,53 \times 10^6\ \text{chu kỳ/năm}} = 23,7\ \text{năm} \quad (C.9)$$

$$MTTF_d = \frac{23,7\ \text{năm}}{0,1} = 237\ \text{năm} \quad (C.10)$$

Kết quả này đưa ra một $MTTF_d$ cho bộ phận "cao" theo Bảng 5. Các giả thiết này chỉ có hiệu lực đối với một thời gian hoạt động hạn chế là 23,7 năm đối với van.

C.5 Dữ liệu $MTTF_d$ của các bộ phận điện

C.5.1 Quy định chung

Các Bảng C.2 đến Bảng C.7 chỉ ra một số giá trị trung bình điển hình của $MTTF_d$ cho các bộ phận điện tử. Các dữ liệu được rút ra từ cơ sở dữ liệu loạt SN 29 500 [40]. Tất cả các dữ liệu thuộc loại dữ liệu chung. Các cơ sở dữ liệu có thể dùng được (xem bản danh sách không đầy đủ trong thư mục tham

khảo) giới thiệu các giá trị $MTTF_d$ cho các bộ phận điện tử khác nhau. Nếu người thiết kế SRP/CS có các dữ liệu riêng khác tin cậy được về các bộ phận được sử dụng thì nên khuyến khích sử dụng các dữ liệu riêng này.

Các giá trị cho trong các Bảng C.2 đến Bảng C.7 có giá trị đối với nhiệt độ 40 ^{0}C, tải danh định của dòng điện và điện áp.

Trong cột $MTTF_d$ của các Bảng, các giá trị từ SN 29 500 dùng cho các bộ phận chung đối với tất cả các dạng hư hỏng có thể có, không nhất thiết phải là các hư hỏng nguy hiểm. Trong cột $MTTF_d$, có thể giả thiết rằng không phải tất cả các dạng hư hỏng đều dẫn đến hư hỏng nguy hiểm. Điều này phụ thuộc chủ yếu vào ứng dụng. Phương pháp chính xác để xác định $MTTF_d$ "điển hình" cho các bộ phận là thực hiện một FMEA. Một số bộ phận hoặc linh kiện, ví dụ, các tranzito được sử dụng như các công tắc có thể có sự ngắn mạch hoặc ngắt mạch do hư hỏng. Chỉ một trong hai dạng hư hỏng này có thể là dạng hư hỏng nguy hiểm; do đó cột "ghi chú" giả thiết chỉ có 50 % hư hỏng nguy hiểm, nghĩa là $MTTF_d$ cho các bộ phận bằng hai lần giá trị MTTF đã cho. Đối với sử dụng, khi có sự nghi ngờ, $MTTF_d$ trong trường hợp xấu nhất đối với các bộ phận được cho trong cột $MTTF_d$ "trường hợp xấu nhất", ở đây hệ số an toàn là 10.

C.5.2 Bán dẫn

Xem các Bảng C.2 và Bảng C.3.

Bảng C.2 – Tranzito (được dùng như công tắc)

Tranzito	Ví dụ	MTTF cho các linh kiện năm	$MTTF_d$ cho các linh kiện năm		Ghi chú
			Điển hình	Trường hợp xấu nhất	
Hai cực	TO18, TO92 SOT23	34 247	68 493	6 849	50 % hư hỏng nguy hiểm
Hai cực, công suất thấp	TO5, TO39	5 708	11 416	1 142	50 % hư hỏng nguy hiểm
Hai cực, công suất	TO3, TO220 D – Pack	1 941	3 881	388	50 % hư hỏng nguy hiểm
FET	Junction MOS	22 831	45 662	4 506	50 % hư hỏng nguy hiểm
MOS công suất	TO3, TO220 D- Pack	1 142	2 283	228	50 % hư hỏng nguy hiểm

Bảng C.3 – Điôt, bán dẫn công suất và mạch tích hợp

Điôt	Ví dụ	MTTF cho các linh kiện năm	$MTTF_d$ cho các linh kiện năm		Ghi chú
			Điển hình	Trường hợp xấu nhất	
Thông dụng	–	114 155	228 311	22 831	50 % hư hỏng nguy hiểm
Triệt	–	15 981	31 963	3 196	50 % hư hỏng nguy hiểm
Điôt Zenen $P_{tot} < 1$ W	–	114 155	228 311	22 831	50 % hư hỏng nguy hiểm
Điôt chỉnh lưu	–	57 078	114 155	11 416	50 % hư hỏng nguy hiểm
Cầu chỉnh lưu	–	11 415	22 831	2 283	50 % hư hỏng nguy hiểm
Thyristo	–	2 283	4 566	457	50 % hư hỏng nguy hiểm
Triac, Diac	–	1 484	2 968	297	50 % hư hỏng nguy hiểm
Mạch tích hợp (lập trình được và không lập trình được)	Sử dụng dữ liệu của nhà sản xuất				50 % hư hỏng nguy hiểm

C.6 Linh kiện thụ động

Xem các Bảng C.4 đến Bảng C.7.

Bảng C.4 – Tụ điện

Tụ điện	Ví dụ	MTTF cho các linh kiện năm	$MTTF_d$ cho các linh kiện, năm		Ghi chú
			Điển hình	Trường hợp xấu nhất	
Tiêu chuẩn, không công suất	KS, KP, KC, KT, MKT, MKC MKP, MKU, MP, MKV	57 078	114 155	11 416	50 % hư hỏng nguy hiểm
Gốm	–	22 831	45 662	4 566	50 % hư hỏng nguy hiểm
Điện phân nhôm	Chất điện phân không rắn	22 831	45 662	4 566	50 % hư hỏng nguy hiểm
Điện phân nhôm	Chất điện phân rắn	37 671	75 342	7 534	50 % hư hỏng nguy hiểm
Điện phân tantali	Chất điện phân không rắn	11 415	22 831	2 283	50 % hư hỏng nguy hiểm
Điện phân tantali	Chất điện phân rắn	114 155	228 311	22 831	50 % hư hỏng nguy hiểm

Bảng C.5 – Điện trở

Điện trở	Ví dụ	MTTF cho các linh kiện năm	$MTTF_d$ cho các linh kiện năm		Ghi chú
			Điển hình	Trường hợp xấu nhất	
Màng cacbon	–	114 155	228 311	22 831	50 % hư hỏng nguy hiểm
Màng kim loại	–	570 776	1 141 552	114 155	50 % hư hỏng nguy hiểm
Oxit kim loại và dây quấn	–	22 831	45 662	4 566	50 % hư hỏng nguy hiểm
Biến đổi	–	3 767	7 534	753	50 % hư hỏng nguy hiểm

Bảng C.6 – Cuộn cảm

Điện trở	Ví dụ	MTTF cho các linh kiện năm	$MTTF_d$ cho các linh kiện năm		Ghi chú
			Điển hình	Trường hợp xấu nhất	
Cho ứng dụng MC	–	37 671	75 342	7 534	50 % hư hỏng nguy hiểm
Cuộn cảm tần số thấp và máy biến áp	–	22 831	45 662	4 566	50 % hư hỏng nguy hiểm
Biến áp lực và biến áp cho chế độ chuyển mạch và cung cấp công suất	–	11 415	22 831	2 283	50 % hư hỏng nguy hiểm

Bảng C.7 – Optocoupler (được dùng như bộ ghép quang)

Opto coupler	Ví dụ	MTTF cho các linh kiện năm	$MTTF_d$ cho các linh kiện năm		Ghi chú
			Điển hình	Trường hợp xấu nhất	
Đầu ra hai cực	SFH 610	7 648	15 296	1 530	50 % hư hỏng nguy hiểm
Đầu ra FET	LH 1056	2 854	5 708	571	50 % hư hỏng nguy hiểm

Phụ lục D
(Tham khảo)

Phương pháp đơn giản hoá để dự tính $MTTF_d$ cho mỗi kênh

D.1 Phương pháp đếm các bộ phận

Sử dụng "phương pháp đếm các bộ phận" để dự tính $MTTF_d$ cho mỗi kênh riêng biệt. Các giá trị của $MTTF_d$ của tất cả các bộ phận đơn, là một phần của kênh, được sử dụng trong tính toán này[4)].

Công thức chung là

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\bar{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\bar{N}} \frac{n_j}{MTTF_{dj}} \qquad (D.1)$$

trong đó

$MTTF_d$ là của toàn bộ kênh;

$MTTF_{di}$, $MTTF_{dj}$ là $MTTF_d$ của mỗi bộ phận đã có đóng góp vào chức năng an toàn.

Tổng đầu tiên là của mỗi bộ phận riêng biệt; tổng thứ hai là một tổng tương đương, có dạng đơn giản hoá trong đó có tất cả các bộ phận giống nhau n_j có cùng một $MTTF_d$ được tập hợp thành nhóm với nhau.

Ví dụ cho trong Bảng D.1 đưa ra một $MTTF_d$ của kênh 21,4 năm, đó là kênh "trung bình" theo Bảng 5.

Bảng D.1 – Ví dụ về danh sách các linh kiện của một bảng mạch

j	Linh kiện	n_j	$MTTF_{dj}$ Trường hợp xấu nhất năm	$1/MTTF_{dj}$ Trường hợp xấu nhất 1/năm	$n_j/MTTF_{dj}$ Trường hợp xấu nhất 1/năm
1	Tranzito, 2 cực, công suất thấp (xem Bảng C.2)	2	1 142	0,000 876	0,001 752
2	Điện trở, màng cacbon (xem Bảng C.5)	5	22 831	0,000 044	0,000 219
3	Tụ, tiêu chuẩn, không công suất (xem Bảng C.4)	4	11 416	0,000 088	0,000 350
4	Rơle (có tải trọng nhỏ, xem C.2) (B_{10d}=20 000 000 chu kỳ, n_{op} = 633 600)	4	315,66	0,003 168	0,012 672
5	Công tắc tơ (có tải trọng danh nghĩa, xem C.2) (B_{10d} = 2 000 000 chu kỳ, n_{op} = 633 600)	1	31,57	0,031 676	0,031 676
$\Sigma(n_j/MTTF_{dj})$					0,046 669
$MTTF_d = 1/\Sigma(n_j/MTTF_d)$ [năm]					21,43

[4)] Phương pháp đếm các bộ phận là phương pháp gần đúng nên luôn có sai số về mặt an toàn. Nếu cần có các giá trị chính xác hơn, người thiết kế nên tính đến các dạng hư hỏng, nhưng điều này có thể rất phức tạp.

CHÚ THÍCH 1: Phương pháp này dựa trên giả thiết là một hư hỏng nguy hiểm của bất cứ linh kiện nào trong một kênh sẽ dẫn tới hư hỏng nguy hiểm của kênh. Việc tính toán $MTTF_d$ như đã minh hoạ trong Bảng D.1 dựa trên giả thiết này.

CHÚ THÍCH 2: Trong ví dụ này, ảnh hưởng chính đến từ công tắc tơ. Các giá trị được lựa chọn cho $MTTF_d$ và B_{10d} cho ví dụ này dựa trên Phụ lục C. Để ứng dụng, giả thiết dop = 220 ngày/năm, h_{op} = 8 h/ngày và t_{cycle} = 10 s/chu kỳ sẽ có n_{op} = 633 600 chu kỳ/năm. Thông thường, khi lấy các giá trị của nhà sản xuất cho $MTTF_d$ và B_{10d} sẽ dẫn đến kết quả tốt hơn nhiều, đó là một $MTTF_d$ cao hơn đối với kênh.

D.2 $MTTF_d$ cho các kênh khác nhau, sự đối xứng hoá của $MTTF_d$ cho mỗi kênh

Các cấu trúc lựa chọn của 6.2 giả thiết rằng đối với các kênh khác nhau trong một SRP/CS dư thừa thì các giá trị của $MTTF_d$ đối với mỗi kênh là như nhau. Giá trị này cho một kênh nên được nhập vào Hình 5.

Nếu $MTTF_d$ của các kênh khác nhau, sẽ có hai khả năng

- Trong trường hợp được giả thiết là xấu nhất, nên tính đến giá trị thấp hơn;
- Có thể sử dụng phương trình D.2 để dự tính một giá trị có thể thay thế cho $MTTF_d$ của mỗi kênh

$$MTTF_d = \frac{2}{3}\left[MTTF_{d\,C1} + MTTF_{d\,C2} - \frac{1}{\frac{1}{MTTF_{d\,C1}} + \frac{1}{MTTF_{d\,C2}}} \right] \qquad (D.2)$$

trong đó $MTTF_{dc1}$ và $MTTF_{dc2}$ là các giá trị cho hai kênh dư thừa khác nhau.

VÍ DỤ Một kênh có $MTTF_{dc1}$ = 3 năm, một kênh khác có $MTTF_{dc2}$ = 100 năm thì $MTTF_d$ tương đương cho mỗi kênh là 66 năm. Điều này có nghĩa là một hệ thống dư thừa có $MTTF_d$ bằng 100 năm trong một kênh và $MTTF_d$ bằng 3 năm trong một kênh khác sẽ bằng một hệ thống trong đó mỗi kênh có $MTTF_d$ bằng 66 năm.

Một hệ thống dư thừa có hai kênh và các giá trị $MTTF_d$ khác nhau đối với mỗi kênh có thể được thay bằng một hệ thống dư thừa có $MTTF_d$ giống nhau trong mỗi kênh bằng cách sử dụng công thức trên. Phương pháp này là cần thiết để sử dụng đúng Hình 5.

CHÚ THÍCH: Phương pháp này giả thiết các kênh độc lập song song.

Phụ lục E

(Tham khảo)

Các dự tính cho vùng chẩn đoán (DC) đối với các chức năng và mô đun

E.1 Các ví dụ của vùng chẩn đoán

Xem Bảng E.1.

Bảng E.1 – Các dự tính cho vùng chẩn đoán

Biện pháp	DC
Thiết bị nhập	
Kích thích thử nghiệm có chu kỳ bằng sự thay đổi động của các tín hiệu nhập	90 %
Kiểm tra tính hợp lý, ví dụ các công tắc thường mở và thường đóng liên kết cơ khí	99 %
Giám sát chéo các tín hiệu nhập không qua thử nghiệm động	0 % đến 99 % tuỳ thuộc vào cách thay đổi của một tín hiệu được thực hiện bởi ứng dụng
Giám sát chéo các tín hiệu nhập có thử nghiệm động nếu không phát hiện được ngắn mạch (đối với I/O đa dữ liệu)	90 %
Giám sát chéo các tín hiệu nhập và các kết quả trung gian trong hệ thống logic (L) và thiết bị kiểm soát phần mềm logic và tức thời của dòng chương trình và phát hiện lỗi tĩnh và ngắn mạch (đối với I/O đa dữ liệu)	99 %
Giám sát gián tiếp (ví dụ, giám sát bằng công tắc áp suất, giám sát vị trí bằng điện của cơ cấu dẫn động)	90 % đến 99 % tuỳ thuộc vào ứng dụng
Giám sát trực tiếp (ví dụ, giám sát vị trí bằng điện của các van điều khiển, giám sát các thiết bị điện cơ bằng các phần tử tiếp xúc liên kết cơ khí)	99 %
Phát hiện lỗi bằng quá trình	0 % đến 99 % tuỳ thuộc vào ứng dụng; chỉ riêng biện pháp này là không đủ đối với mức tính năng e!
Giám sát một số đặc tính của cảm biến (thời gian đáp ứng, dải các tín hiệu analog, ví dụ, điện trở, điện dung)	60 %

Bảng E.1 – (tiếp theo)

Biện pháp	DC
Logic	
Giám sát gián tiếp (ví dụ, giám sát bằng công tắc áp suất, giám sát bằng điện của cơ cấu dẫn động (tác động)	90 % đến 99 %, tuỳ thuộc vào ứng dụng
Giám sát trực tiếp (ví dụ, giám sát vị trí bằng điện của các van điều khiển, giám sát các thiết bị điện - cơ bằng các phần tử tiếp xúc liên kết cơ khí)	99 %
Giám sát thời gian tức thời đơn giản của mạch logic (ví dụ, bộ đo thời gian kiểu đồng hồ kiểm soát, trong đó có các điểm trigơ ở trong chương trình của hệ thống logic)	60 %
Giám sát tức thời và lôgic của mạch lôgic bằng đồng hồ kiểm soát, trong đó thiết bị thử nghiệm thực hiện các kiểm tra tính hợp lý của trạng thái hệ thống logic	90 %
Các phép tự kiểm tra khởi động để phát hiện các lỗi tiềm ẩn trong các bộ phận của hệ thống logic (ví dụ, chương trình và các bộ nhớ dữ liệu, các cổng nhập/xuất, các giao diện)	90 % (tuỳ thuộc vào kỹ thuật kiểm tra)
Kiểm khả năng phản ứng của thiết bị giám sát (ví dụ, đồng hồ kiểm soát) bằng kênh chính tại lúc khởi động hoặc khi nào có yêu cầu đối với chức năng an toàn hoặc khi nào một tín hiệu bên ngoài cần đến nó thông qua một thiết bị nhập	90 %
Nguyên tắc động (tất cả các linh kiện của mạch logic được yêu cầu để thay đổi trạng thái ON - OFF - ON khi cần đến chức năng an toàn) ví dụ, mạch khoá liên động được thực hiện bởi các rơle	99 %
Bộ nhớ không thay đổi: chữ ký một từ (8 bít)	90 %
Bộ nhớ không thay đổi: chữ ký từ kép (16 bít)	99 %
Bộ nhớ thay đổi: kiểm tra RAM bằng cách sử dụng dữ liệu dư thừa ví dụ, cờ, dấu hiệu, hằng số, bộ đo thời gian và so sánh chéo các dữ liệu này	60 %
Bộ nhớ thay đổi: kiểm khả năng đọc và khả năng ghi của ô chứa dữ liệu của bộ nhớ được sử dụng	60 %
Bộ nhớ thay đổi: kiểm soát RAM với mã tự chỉnh cải tiến hoặc tự kiểm tra RAM (ví d ụ, "galpat" hoặc "Abraham")	99 %
Đơn v ị xử lý: tự kiểm tra bằng phần mềm	60 % đến 90 %
Đơn vị xử lý: xử lý được mã hoá	90 % đến 99 %

Bảng E.1 – (kết thúc)

Biện pháp	DC
Phát hiện lỗi bằng quá trình	0 % đến 99 %, tuỳ thuộc vào ứng dụng; chỉ riêng biện pháp này là không đủ đối với mức tính năng yêu cầu "e"
Thiết bị xuất	
Giám sát các tín hiệu xuất bởi một kênh không có thử nghiệm động	0 % đến 99 % tuỳ thuộc vào cách thay đổi của một tín hiệu được thực hiện bởi ứng dụng
Giám sát chéo các tín hiệu xuất không có thử nghiệm động	0 % đến 99 % tuỳ thuộc vào cách thay đổi của một tín hiệu được thực hiện bởi ứng dụng
Giám sát chéo các tín hiệu xuất có thử nghiệm động không phát hiện ngắn mạch (đối với I/O đa dữ liệu)	90 %
Giám sát chéo các tín hiệu xuất và các kết quả trung gian trong hệ thống logic (L) và thiết bị kiểm soát phần mềm logic tức thời của dòng chương trình và phát hiện các lỗi tĩnh và ngắn mạch (đối với I/O đa dữ liệu)	99 %
Đường dẫn ngưng dư thừa không có sự giám sát cơ cấu dẫn động (tác động)	0 %
Đường dẫn ngưng dư thừa có sự giám sát một trong các cơ cấu dẫn động (tác động) bằng hệ thống logic hoặc thiết bị thử nghiệm	90 %
Đường dẫn ngưng dư thừa có sự giám sát một trong các cơ cấu dẫn động (tác động) bằng hệ thống logic hoặc thiết bị thử nghiệm	99 %
Giám sát gián tiếp (ví dụ, giám sát bằng công tắc áp suất, giám sát vị trí bằng điện của các cơ cấu dẫn động)	90 % đến 99 %, tuỳ thuộc vào ứng dụng
Phát hiện lỗi bằng tiến trình	0 % đến 99 %, tuỳ thuộc vào ứng dụng; chỉ riêng biện pháp này là không đủ đối với mức tính năng e
Giám sát trực tiếp (ví dụ, giám sát vị trí bằng điện của các van, giám sát các thiết bị điện - cơ bằng các phần tử tiếp xúc liên kết cơ khí)	99 %
CHÚ THÍCH 1: Đối với các dự tính bổ sung cho DC, xem, ví dụ IEC 61508-2:2000, các Bảng A.2 đến Bảng A.15. CHÚ THÍCH 2: Nếu hệ thống logic đòi hỏi DC trung bình hoặc cao thì ít nhất phải áp dụng một biện pháp cho bộ nhớ thay đổi, bộ nhớ không thay đổi và bộ xử lý có các DC tối thiểu là 60 %.	

E.2 Dự tính DC trung bình (DC_{avg})

Trong nhiều hệ thống, có thể sử dụng nhiều biện pháp để phát hiện lỗi. Các biện pháp này có thể kiểm các phần khác nhau của SRP/CS và có các DC khác nhau. Để dự tính mức tính năng (PL) theo Hình 5 thì chỉ áp dụng một DC trung bình cho toàn bộ SRP/CS thực hiện chức năng an toàn.

Có thể xác định DC là tỷ số giữa tần suất hư hỏng của các hư hỏng nguy hiểm được phát hiện và tần suất của tổng các hư hỏng nguy hiểm. Theo định nghĩa này, vùng chẩn đoán trung bình DC_{avg} được dự tính theo công thức sau:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + ... + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + ... + \frac{1}{MTTF_{dN}}} \quad \text{(E.1)}$$

Ở đây phải xem xét và lấy tổng của các thành phần của SRP/CS không có sự ngăn chặn lỗi. Đối với mỗi khối cần tính đến $MTTF_d$ và DC. DC trong công thức này có nghĩa là tỷ số giữa tần suất hư hỏng của các hư hỏng nguy hiểm được phát hiện của phần cấu thành (bỏ qua các biện pháp dùng để phát hiện hư hỏng) và tần suất hư hỏng của tất cả các hư hỏng nguy hiểm của phần cấu thành đó. Vì vậy, DC có liên quan đến phần cấu thành được thử nghiệm và không liên quan đến thiết bị thử nghiệm. Các thành phần của SRP/CS không phát hiện ra lỗi (ví dụ, các thành phần không được thử nghiệm) có DC = 0 và chỉ đóng góp vào mẫu số của DC_{avg}.

Phụ lục F
(Tham khảo)

Dự tính đối với hư hỏng do nguyên nhân chung (CCF)

F.1 Yêu cầu đối với CCF

Một thủ tục toàn diện dùng cho các biện pháp phòng tránh CCF đối với các cảm biến/cơ cấu dẫn động (tác động) và tách rời khỏi mạch logic điều khiển được giới thiệu trong IEC 61508-6:2000, Phụ lục D. Không phải tất cả các biện pháp được cho ở đây đều áp dụng được cho máy. Ở đây chỉ đưa ra các biện pháp quan trọng nhất.

CHÚ THÍCH: Trong tiêu chuẩn này, giả thiết rằng đối với các hệ thống dư thừa, hệ số β theo IEC 61508-6:2000, Phụ lục D nên nhỏ hơn hoặc bằng 2 %.

F.2 Dự tính ảnh hưởng của CCF

Quá trình định lượng này nên được tiến hành cho toàn bộ hệ thống. Mỗi phần cấu thành của các bộ phận liên quan đến an toàn của hệ thống điều khiển nên được xem xét.

Bảng F.1 liệt kê các biện pháp và chứa các giá trị gắn liền với các biện pháp dựa trên cơ sở đánh giá về mặt kỹ thuật sự đóng góp của mỗi biện pháp vào việc giảm hư hỏng do nguyên nhân chung.

Đối với mỗi biện pháp đã được liệt kê, chỉ có thể cho toàn bộ số điểm hoặc không có điểm nào. Nếu một biện pháp chỉ được thực hiện một phần thì số điểm cho biện pháp này là không điểm (zero).

Bảng F.2 đưa ra sự định lượng CCF.

Bảng F.1 – Quá trình cho điểm và định lượng các biện pháp phòng tránh CCF

TT	Biện pháp phòng tránh CCF	Điểm
1	Tách biệt/tách rời	
	Tách biệt về vật lý giữa các đường dẫn tín hiệu: tách biệt trong đường dây/đường (ống) dẫn khe hở thích hợp và khoảng cách để phòng lão hoá trên bảng mạch in	15
2	Tách đa dạng	
	Các công nghệ/thiết kế khác nhau hoặc các nguyên tắc vật lý được sử dụng, ví dụ: kênh điện tử lập trình thứ nhất và kênh thứ hai được gắn cứng, loại khởi tạo, áp suất và nhiệt độ Đo khoảng cách và áp suất số và analog Các bộ phận (linh kiện) của sản xuất khác nhau	20

Bảng F.1 – (kết thúc)

STT	Biện pháp phòng tránh CCF	Điểm
3	Thiết kế/ứng dụng/kinh nghiệm	
3.1	Bảo vệ tránh quá điện áp, quá áp suất, quá dòng điện, v.v...	15
3.2	Các bộ phận (linh kiện) được sử dụng là đã quen và đáng tin cậy	5
4	Đánh giá/phân tích	
	Các kết quả của một dạng hư hỏng và phân tích ảnh hưởng có được tính đến hay chưa để tránh hư hỏng do nguyên nhân chung trong thiết kế	5
5	Kỹ năng/huấn luyện	
	Người thiết kế/người bảo dưỡng đã được huấn luyện, đào tạo để hiểu được các nguyên nhân và hậu quả của các hư hỏng do nguyên nhân chung chưa?	5
6	Môi trường	
6.1	Sự phòng ngừa nhiễm bẩn và tính tương thích điện từ (EMC) tránh CCF theo các tiêu chuẩn thích hợp. Hệ thống chất lỏng: sự lọc môi trường có áp suất, ngăn ngừa sự thâm nhập của chất bẩn, xả không khí bị nén, ví dụ, phù hợp với các yêu cầu của nhà sản xuất bộ phận về độ sạch của môi trường có áp Hệ thống điện: hệ thống đã được kiểm về tính miễn dịch điện từ chưa?, ví dụ theo quy định trong các tiêu chuẩn có liên quan để tránh CCF Đối với các hệ thống thuỷ lực và điện kết hợp cần xem xét cả hai khía cạnh thuỷ lực và điện	25
6.2	Các ảnh hưởng khác Các yêu cầu về tính miễn dịch đối với tất cả các ảnh hưởng của môi trường có liên quan như nhiệt độ, va chạm, rung, độ ẩm (ví dụ, như đã quy định trong các tiêu chuẩn có liên quan) đã được xem xét chưa?	10
	Tổng	[lớn nhất đạt được 100]

Tổng số điểm	Các biện pháp phòng tránh CCF[a]
65 hoặc lớn hơn	Đáp ứng các yêu cầu
Nhỏ hơn 65	Quá trình không đạt => chọn các biện pháp bổ sung

[a] Khi không có liên quan đến các biện pháp công nghệ, các điểm được cho theo cột này có thể được xem xét trong tính toán toàn diện.

Phụ lục G

(Tham khảo)

Hư hỏng có hệ thống

G.1 Quy định chung

TCVN 7384-2 (ISO 13849-2) đưa ra danh sách toàn diện các biện pháp phòng tránh hư hỏng có hệ thống nên được áp dụng làm cơ sở và các nguyên tắc an toàn đã quen và đáng tin cậy.

G.2 Các biện pháp để điều khiển các hư hỏng có hệ thống

Cần áp dụng các biện pháp sau

– Sử dụng sự ngắt điện [xem TCVN 7384-2 (ISO 13849-2)]

Các bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS) nên được thiết kế sao cho khi mất nguồn cung cấp điện thì trạng thái an toàn của máy được xác lập và duy trì.

– Các biện pháp để kiểm soát ảnh hưởng của sự mất điện áp, thay đổi điện áp, quá điện áp, điện áp thấp.

Nên xác định trước trạng thái của SRP/CS đáp lại sự mất điện áp, thay đổi điện áp, quá điện áp và điện áp thấp để cho SRP/CS có thể đạt được hoặc duy trì trạng thái an toàn của máy (cũng xem IEC 60204-1 và IEC 61508-7:2000, A.8).

– Các biện pháp để kiểm soát hoặc tránh các ảnh hưởng của môi trường vật lý (ví dụ như, nhiệt độ, độ ẩm, nước, rung, bụi bẩn, chất ăn mòn, nhiễu điện từ và tác dụng của nó).

Nên xác định trước trạng thái của SRP/CS đáp lại các ảnh hưởng của môi trường vật lý để cho SRP/CS có thể đạt được hoặc duy trì được trạng thái an toàn của máy (xem, ví dụ như IEC 60529, IEC 60204-1).

– Phải sử dụng giám sát sự tuần tự của chương trình với SRP/CS chứa phần mềm để phát hiện ra các trình tự chương trình có sai sót. Một trình tự chương trình có sai sót xảy ra nếu các thành phần riêng của một chương trình (ví dụ, các môđun phần mềm, các chương trình con hoặc các lệnh) được xử lý theo trình tự sai hoặc chu kỳ thời gian hoặc nếu đồng hồ của bộ xử lý sai (xem EN 61508-7:2001, A.9).

– Các biện pháp để kiểm soát các ảnh hưởng của sai số và các ảnh hưởng khác xuất hiện từ bất cứ quá trình thông tin liên lạc dữ liệu nào (xem IEC 61508-2:2000, 7.4.8).

Ngoài ra nên áp dụng một hoặc nhiều biện pháp sau, có tính đến độ phức tạp của SRP/CS và mức tính năng (PL) của nó:

- Phát hiện hư hỏng bằng các thử nghiệm tự động;
- Các thử nghiệm bằng phần cứng có dư thừa;
- Các kiểu phần cứng khác nhau;
- Vận hành ở chế độ dương;
- Các công tắc liên kết cơ khí;
- Tác động mở trực tiếp;
- Chế độ định hướng hư hỏng;
- Xác định kích thước quá mức bằng một hệ số thích hợp, trong đó nhà sản xuất có thể chứng minh rằng sự giảm công suất sẽ cải thiện độ tin cậy – khi sự xác định kích thước quá mức là thích hợp, nên sử dụng hệ số xác định kích thước quá mức tối thiểu là 1,5.

Xem TCVN 7384-2:2010 (ISO 13849-2:2003), D.3.

G.3 Các biện pháp để phòng tránh hư hỏng có hệ thống

Nên áp dụng các biện pháp sau

- Sử dụng các vật liệu thích hợp và gia công phù hợp

Lựa chọn vật liệu, các phương pháp gia công và nhiệt luyện có liên quan đến ứng suất, tuổi thọ, độ đàn hồi, ma sát, mài mòn, ăn mòn, nhiệt độ, độ dẫn (điện, nhiệt), độ bền điện môi.

- Xác định kích thước và hình dạng đúng

Cần xem xét đến ứng suất, biến dạng, mỏi, nhiệt độ, nhám bề mặt, dung sai, sự gia công chế tạo.

- Lựa chọn đúng, tổ hợp, gá đặt, lắp ráp và lắp đặt các bộ phận, bao gồm cả sự đặt cáp, đường dây và bất cứ sự nối ghép hoặc hợp mạng nào.

Áp dụng các tiêu chuẩn thích hợp, và hướng dẫn áp dụng của nhà sản xuất, ví dụ, các tờ catalog, hướng dẫn lắp đặt, điều kiện kỹ thuật và sử dụng quy trình kỹ thuật tốt.

- Tính tương thích

Sử dụng các bộ phận có đặc tính làm việc tương thích

- Chịu được các điều kiện quy định về môi trường

Thiết kế SRP/CS sao cho có khả năng làm việc trong tất cả các môi trường yêu cầu và trong bất cứ điều kiện không thuận lợi thấy trước nào, ví dụ, nhiệt độ, độ ẩm, rung và nhiễu điện từ (EMI) [xem TCVN 7384-2:2010 (ISO 13849-2:2003), D.2].

– Sử dụng các bộ phận được thiết kế theo một tiêu chuẩn thích hợp và các dạng hư hỏng dễ nhận ra

Giảm rủi ro các lỗi không được phát hiện bằng cách sử dụng các bộ phận có đặc tính riêng (xem IEC 61508-7:2000, B.3.3).

Ngoài ra nên áp dụng một hoặc nhiều các biện pháp sau, có tính đến độ phức tạp của SRP/CS và mức tính năng (PL) của nó.

– Xem xét lại thiết kế phần cứng (ví dụ, bằng cách kiểm tra hoặc bước chuyển đến)

Phát hiện bằng các xem xét và phân tích các sự khác biệt giữa điều kiện kỹ thuật (đặc tính kỹ thuật) và sự thực hiện (IEC 61508-7:2000. B.3.7 và B.3.8).

– Các công cụ thiết kế có sự trợ giúp của máy tính có khả năng mô phỏng và phân tích

Thực hiện quy trình thiết kế có hệ thống và bao gồm các thành phần cấu trúc tự động thích hợp sẵn có cho sử dụng và thử nghiệm (xem IEC 61508-7:2000, B.3.5).

– Mô phỏng

Thực hiện việc kiểm tra đầy đủ và có hệ thống một thiết kế SRP/CS dưới dạng đặc tính chức năng làm việc và xác định kích thước đúng của các thành phần của chúng (IEC 61508-7:2000, B.3.6).

G.4 Các biện pháp phòng tránh các hư hỏng có hệ thống trong quá trình tích hợp SRP/CS

Nên áp dụng các biện pháp sau trong quá trình tích hợp SRP/CS

– Thử nghiệm chức năng;

– Quản lý đề án thiết kế;

– Lập tài liệu

Ngoài ra nên áp dụng thử nghiệm hộp đen, có tính đến độ phức tạp của SRP/CS và mức tính năng (PL) của nó.

Phụ lục H

(Tham khảo)

Ví dụ về tổ hợp nhiều bộ phận liên quan đến an toàn của hệ thống điều khiển

Hình H.1 là một sơ đồ của các bộ phận liên quan đến an toàn cung cấp một trong các chức năng điều khiển một cơ cấu chấp hành (tác động) của máy. Đây không phải là một sơ đồ chức năng/làm việc và chỉ được dùng để chứng minh nguyên tắc phối hợp các loại và các công nghệ trong một chức năng.

Việc điều khiển được thực hiện thông qua hệ thống logic điều khiển điện tử và một van thuỷ lực phân phối. Rủi ro được giảm đi bởi một thiết bị bảo vệ quang điện tử phóng xạ (AOPD) phát hiện sự tiếp cận tình trạng nguy hiểm và ngăn ngừa sự khởi động của cơ cấu chấp hành thuỷ lực khi chùm sáng bị ngắt.

Các bộ phận liên quan đến an toàn cung cấp chức năng an toàn là: AOPD, hệ thống logic điều khiển điện tử, van phân phối thuỷ lực và các phương tiện nối.

Các bộ phận liên quan đến an toàn tổ hợp này cung cấp một chức năng dừng như một chức năng an toàn. Vì AOPD được ngắt, các đầu ra truyền một tín hiệu cho hệ thống logic điều khiển điện tử, hệ thống logic này cung cấp một tín hiệu cho van phân phối thuỷ lực để dừng dòng thuỷ lực với tư cách là đầu ra của SRP/CS. Ở máy, quá trình này dừng chuyển động nguy hiểm của cơ cấu chấp hành.

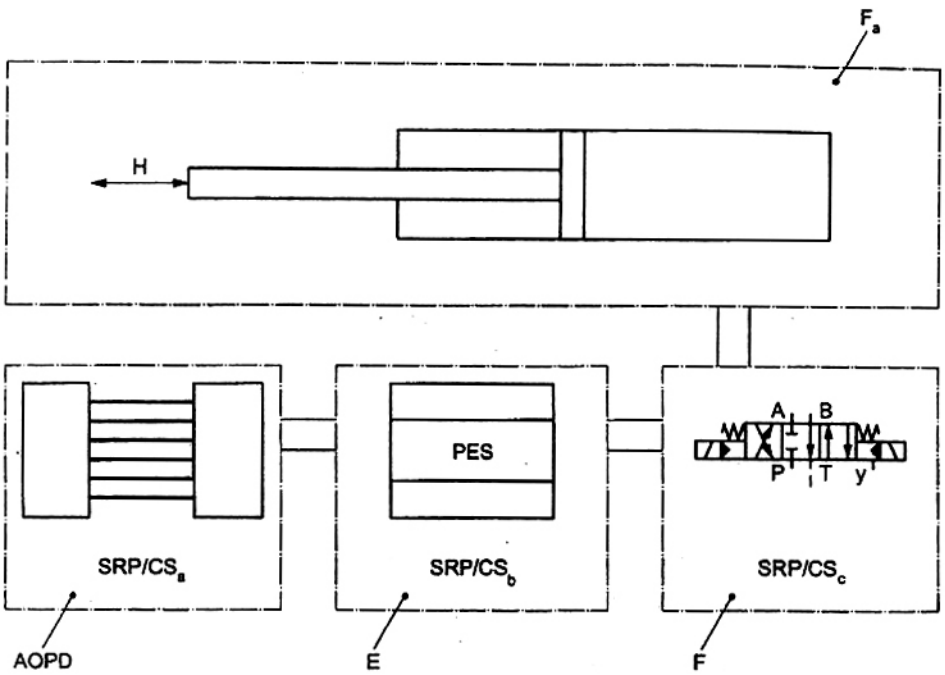
Tổ hợp này của các bộ phận liên quan đến an toàn tạo ra một chức năng an toàn biểu thị sự phối hợp của các loại và công nghệ khác nhau dựa trên các yêu cầu cho trong Điều 6. Khi sử dụng các nguyên tắc cho trong tiêu chuẩn này, có thể mô tả các bộ phận liên quan đến an toàn chỉ ra trên Hình H.2 như sau

- Loại 2, PL = c đối với các thiết bị bảo vệ nhạy cảm điện (hàng rào ánh sáng). Để giảm xác suất xảy ra lỗi, bộ phận này sử dụng các nguyên tắc an toàn đã quen – đáng tin cậy;
- Loại 3, PL = d đối với các hệ thống logic điều khiển điện tử. Để tăng mức tính năng an toàn của hệ thống logic điều khiển điện tử này thì cấu trúc SRP/CS này là dư thừa và thực hiện nhiều biện pháp phát hiện lỗi sao cho có thể phát hiện được hầu hết các lỗi đơn;
- Loại 1, PL = c đối với các van phân phối thủy lực. Trạng thái đã quen – đáng tin cậy được ứng dụng chủ yếu. Trong ví dụ này, van được xem là đã quen – đáng tin cậy. Để giảm xác suất xảy ra lỗi, thiết bị này gồm có các bộ phận đã quen - đáng tin cậy áp dụng các nguyên tắc an toàn đã quen - đáng tin cậy và cần xem xét tất cả các điều kiện ứng dụng (xem 6.2.4).

CHÚ THÍCH 1: Cần tính đến vị trí, kích thước và sự lắp đặt các phương tiện nối.

Tổ hợp này đưa PL_{low} = c và N_{low} = 2 tới một mức tính năng toàn bộ pf PL = c (xem 6.3).

CHÚ THÍCH 2: Trong trường hợp có một lỗi đối với các bộ phận loại 1 hoặc loại 2 của Hình H.2 thì có thể làm mất đi chức năng an toàn.



CHÚ DẪN:

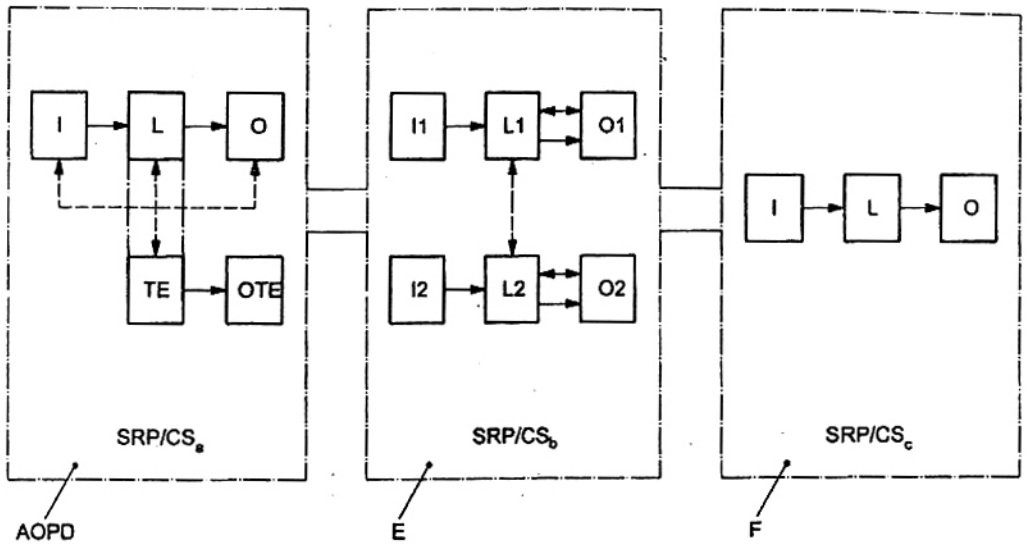
AOPD thiết bị bảo vệ quang điện tử phóng xạ (ví dụ, hàng rào ánh sáng), SRP/CS_a: Loại 2 [kiểu 2], PL = c

E hệ thống logic điều khiển điện tử, SRP/CS_b: Loại 3, PL = d

F cơ cấu chấp hành thuỷ lực

H chuyển động nguy hiểm

Hình H.1 – Ví dụ - Sơ đồ khối giải thích tổ hợp của các SRP/CS



CHÚ DẪN

AOPD	thiết bị bảo vệ quang điện tử phóng xạ (ví dụ, hàng rào ánh sáng)
E	hệ thống logic điều khiển điện tử
F	cơ cấu chấp hành thuỷ lực
I, I1, I2	các thiết bị nhập, ví dụ, cảm biến
L, L1, L2	hệ thống logic
O, O1, O2, OTE	các thiết bị xuất, ví dụ, công tắc tơ chính
TE	thiết bị thử

Hình H.2 - Sự thay thế của Hình H.1 bằng các cấu trúc lựa chọn

Phụ lục I
(Tham khảo)

Các ví dụ

I.1 Quy định chung

Phụ lục này minh hoạ việc sử dụng các phương pháp đã cho trong các phụ lục trên để nhận biết các chức năng an toàn và xác định mức tính năng (PL); Phụ lục này đưa ra các tính toán định lượng cho hai mạch điều khiển được sử dụng rộng rãi. Đối với quy trình từng bước (quá trình lặp), xem Hình 3.

Khảo sát hai ví dụ khác nhau của các mạch điều khiển A và B, xem các Hình I.1 và Hình I.3. Cả hai mạch minh hoạ đặc tính của cùng một chức năng an toàn khoá liên động của cửa bảo vệ. Ví dụ thứ nhất được lập ra như một kênh của các bộ phận điện cơ có các giá trị $MTTF_d$ cao, trong khi ví dụ thứ hai được cấu thành với hai kênh - một kênh điện – cơ và một kênh điện tử lập trình – bao gồm cả các thử nghiệm, nhưng được cấu thành bởi các bộ phận có $MTTF_d$ thấp.

I.2 Chức năng an toàn và mức tính năng yêu cầu (PL_r)

Đối với cả hai ví dụ, chức năng an toàn khoá liên động của một thiết bị bảo vệ có thể được chọn như sau

Chuyển động nguy hiểm sẽ được dừng lại khi cửa bảo vệ được mở ra (bằng ngừng cung cấp năng lượng của động cơ điện).

Các tham số rủi ro theo phương pháp biểu đồ rủi ro (xem Hình A.1) như sau

- Tính nghiêm trọng của thương tích, S = S2, nghiêm trọng;
- Tần suất và/ hoặc thời gian phơi ra trước mối nguy hiểm, F = F1, hiếm tới ít khi phơi ra và/ hoặc thời gian phơi ngắn;
- Khả năng tránh nguy hiểm, P = P1, có thể tránh được trong các điều kiện riêng.

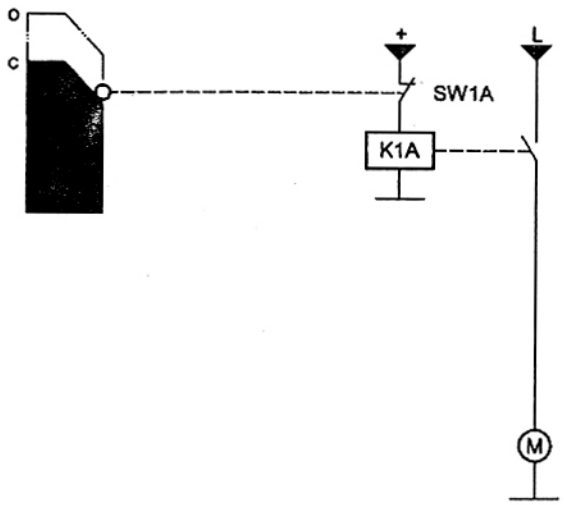
Các quyết định này dẫn đến một mức tính năng yêu cầu PL_r bằng c.

Xác định loại ưu tiên: mức tính năng c có thể đạt được bằng các hệ thống một kênh rất đáng tin cậy (loại 1) hoặc các cấu trúc dư thừa (loại 2 hoặc loại 3) (xem Hình 5 và Điều 6).

I.3 Ví dụ A, hệ thống một kênh

I.3.1 Nhận biết các bộ phận liên quan đến an toàn

Tất cả các bộ phận cấu thành đóng góp vào chức năng an toàn được giới thiệu trên Hình I.1. Bỏ qua các chi tiết chức năng không đóng góp vào chức năng an toàn khoá liên động (như các công tắc khởi động và dừng).



CHÚ DẪN

O mở

C đóng

M động cơ (mô tơ)

K1A công tắc tơ

SW1A công tắc (NC)

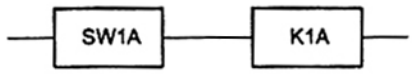
Hình I.1 - Mạch điều khiển A để thực hiện chức năng an toàn

Trong ví dụ này, công tắc cửa có các tiếp điểm thường đóng (nhưng không xem xét đến sự ngăn chặn lỗi) và được nối với công tắc tơ có thể cắt điện đến động cơ:

- Một kênh của các bộ phận điện - cơ;
- Công tắc SW1A có $MTTF_d$ trung bình;
- Công tắc tơ K1A có $MTTF_d$ thấp.

Công tắc tơ được lựa chọn trong ví dụ này là một linh kiện đã quen - đáng tin cậy khi được thực hiện theo TCVN 7384-2 (ISO 13849-2).

Như vậy, các bộ phận liên quan đến an toàn và sự phân chia của chúng thành các kênh có thể được minh hoạ trên sơ đồ khối liên quan đến an toàn như đã chỉ ra trên Hình I.2.



CHÚ DẪN

K1A công tắc tơ

SW1A công tắc

Hình I.2 – Sơ đồ khối liên quan đến an toàn để nhận biết các bộ phận liên quan đến an toàn của ví dụ A

I.3.2 Định lượng $MTTF_d$ đối với mỗi kênh, DC_{avg}, hư hỏng do nguyên nhân chung, loại, PL

Các giá trị $MTTF_d$ đối với mỗi kênh, DC_{avg}, hư hỏng do nguyên nhân chung được giả thiết là được dự tính theo Phụ lục D, C, E và F hoặc do nhà sản xuất cung cấp. Các loại được dự tính theo 6.2.

– $MTTF_d$

Công tắc tơ K1A và công tắc SW1A đóng góp vào $MTTF_d$ của một kênh, $MTTF_{d,\,K1A}$ bằng 50 năm và $MTTF_{d\,SW1A}$ bằng 20 năm được giả thiết là do nhà sản xuất. Phương pháp đếm các bộ phận tạo ra cho $MTTF_d$ của một kênh:

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{SW1A}} + \frac{1}{MTTF_{K1A}} = \frac{1}{20\ \text{năm}} + \frac{1}{50\ \text{năm}} = \frac{0{,}07}{\text{năm}} \qquad (I.1)$$

Phương trình dẫn đến $MTTF_d$ = 14,3 năm hoặc "trung bình" đối với kênh theo 4.5.2, Bảng 5.

CHÚ THÍCH: Nếu không có sẵn thông tin đối với K1A thì có thể giả thiết trường hợp là xấu nhất theo C.2 hoặc C.4.

- DC

Vì không thực hiện thử nghiệm trong mạch điều khiển A cho nên DC = O hoặc "không" theo 4.5.3, Bảng 6.

- Loại

Mặc dù loại ưu tiên đối với mạch này là loại 1, $MTTF_d$ thu được của kênh là "trung bình". Kết quả là chỉ có loại B đạt được bởi thiết kế này.

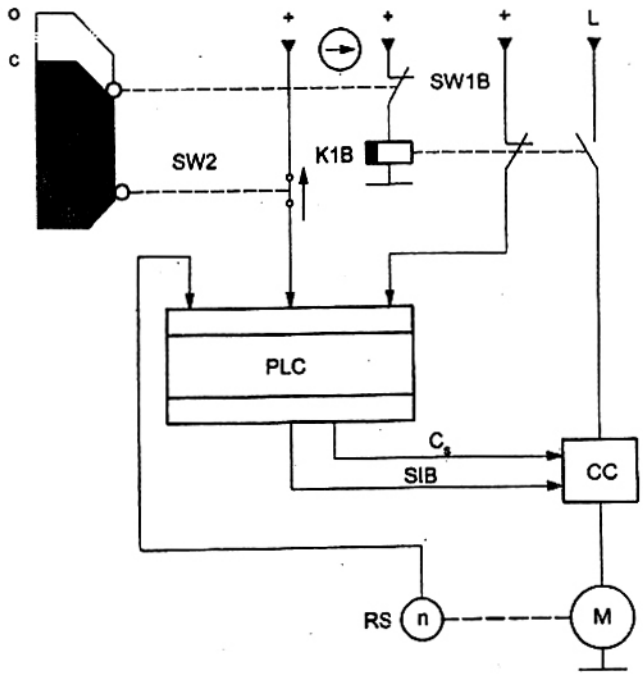
Dữ liệu nhập đối với Hình 5: $MTTF_d$ của mỗi kênh là "trung bình" (14,3 năm), DC_{avg} là "không" và loại là loại B. Kết quả này có thể được xem như đạt mức tính năng b.

Kết quả này không phù hợp với mức tính năng yêu cầu c theo I.2. Như vậy, mạch phải được thiết kế lại và ước lượng lại tới khi đạt mức tính năng c để đáp ứng các yêu cầu về giảm rủi ro của ví dụ trong I.2.

I.4 Ví dụ B, hệ thống dư thừa

I.4.1 Nhận biết các bộ phận liên quan đến an toàn

Tất cả các bộ phận cấu thành đóng góp vào chức năng an toàn được thể hiện trên Hình I.3. Bỏ qua các chi tiết chức năng không đóng góp vào chức năng an toàn khoá liên động (như các công tắc khởi động và dừng hoặc chuyển mạch chậm của K1B).



CHÚ DẪN

PLC bộ điều khiển logic khả lập trình

CC bộ biến dòng

M động cơ (mô tơ)

RS cảm biến quay

O mở

C đóng

Cs chức năng dừng (tiêu chuẩn)

SIB tạo khối xung an toàn

K1B công tắc tơ

SW1B công tắc (NC)

SW2B công tắc (NO)

Hình I.3 - Mạch điều khiển B để thực hiện chức năng an toàn

Trong ví dụ thứ hai này sử dụng hai kênh có sự dư thừa. Kênh thứ nhất tương tự như kênh trong ví dụ A sử dụng một công tắc cửa có tác động mở trực tiếp được dùng ở chế độ vận hành cưỡng bức. Công tắc cửa này được nối với một công tắc tơ có khả năng cắt điện nối với động cơ. Trong kênh thử thứ hai sử dụng các linh kiện điện tử (có khả năng lập trình) bổ sung. Một công tắc cửa thứ hai được nối với một bộ điều khiển logic lập trình có thể điều khiển bộ biến dòng để cắt điện nối với động cơ:

– Các kênh dư thừa, một kênh điện – cơ và một kênh điện tử lập trình;

– Công tắc SW1B có tác động cơ khí cưỡng bức của các tiếp điểm, SW2 có $MTTF_d$ trung bình;

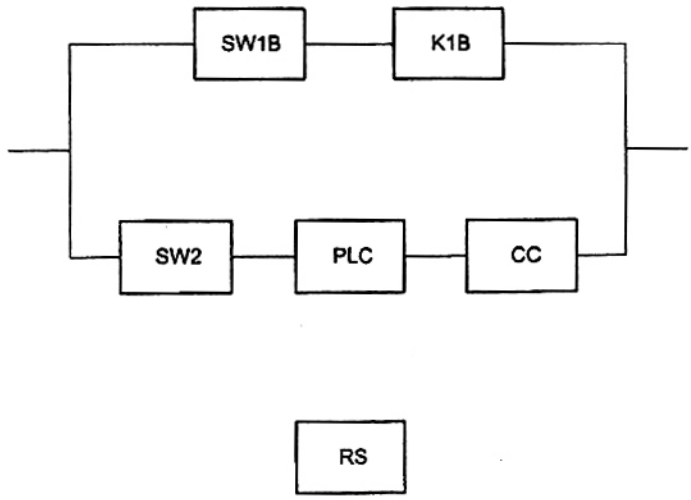
– Công tắc tơ K1B có $MTTF_d$ trung bình, công tắc tơ được lựa chọn trong ví dụ này không phải là linh kiện đã quen - đáng tin cậy;

– Các linh kiện điện tử có $MTTF_d$ trung bình.

Các bộ phận liên quan đến an toàn và sự phân chia chúng thành các kênh có thể được minh hoạ trong sơ đồ khối liên quan đến an toàn như đã chỉ ra trên Hình I.4.

CHÚ THÍCH: Về tính đa dạng của dư thừa, các yêu cầu đối với phần mềm theo 4.6 dùng cho đường dẫn của PLC không được xem là có liên quan.

SW1B và K1B lập ra kênh thứ nhất, SW2, PLC và CC lập ra kênh thứ hai; RS chỉ được dùng để thử nghiệm bộ biến dòng.



CHÚ DẪN

SW1B cơ cấu khoá liên động

K1B công tắc tơ

SW2 công tắc

PLC bộ điều khiển logic lập trình

CC bộ biến dòng

RS cảm biến quay

Hình I.4 – Sơ đồ khối nhận biết các bộ phận liên quan đến an toàn của ví dụ B

I.4.2 Định lượng $MTTF_d$ cho mỗi kênh, DC_{avg}, hư hỏng do nguyên nhân chung, loại và PL

Các giá trị của $MTTF_d$ đối với mỗi kênh, DC_{avg} và hư hỏng do nguyên nhân chung được giả thiết là được dự tính theo các Phụ lục C, D, E và F hoặc do nhà sản xuất cung cấp. Các loại được dự tính theo 6.2.

Công tắc SW1B có tác động mở trực tiếp và được dùng ở chế độ vận hành cưỡng bức. Do đó, sự ngăn chặn lỗi được thực hiện khi một tiếp điểm không mở và công tắc không vận hành do hư hỏng cơ khí (ví dụ, gãy chốt đẩy, mòn cam dẫn động, điều chỉnh sai).

CHÚ THÍCH: Các giả thiết này có giá trị đối với các công tắc của mạch phụ theo IEC 60957-5-1:1997, Phụ lục A, và đối với việc kẹp chặt cơ khí thích hợp và vận hành các công tắc theo điều kiện kỹ thuật của nhà sản xuất [xem TCVN 7384-2 (ISO 13849-2)].

- **$MTTF_d$**

Công tắc tơ K1B chỉ là một thành phần đóng góp vào $MTTF_d$ của một kênh. $MTTF_{K1B}$ bằng 30 năm được giả thiết là do nhà sản xuất đưa ra. Phương pháp đếm các bộ phận của D.1 tạo ra $MTTF_d$ của một kênh.

$$\frac{1}{MTTF_{dC1}} = \frac{1}{MTTF_{dK1B}} \qquad (I.2)$$

Công thức này dẫn đến $MTTF_d$ = 30 năm đối với kênh

Trong kênh thứ hai, SW2, PLC và CC đóng góp vào $MTTF_{dC2}$. Đối với ba linh kiện này cũng như đối với RS, $MTTF_d$ bằng 20 năm được giả thiết là do nhà sản xuất đưa ra. Phương pháp đếm các bộ phận của D.1 tạo ra $MTTF_{dC2}$ của kênh thứ hai

$$\frac{1}{MTTF_{dC2}} = \frac{1}{MTTF_{dSW2}} + \frac{1}{MTTF_{dPLC}} + \frac{1}{MTTF_{dCC}} = \frac{1}{20năm} + \frac{1}{20năm} + \frac{1}{20năm} = \frac{0,15}{năm} \qquad (I.3)$$

Công thức dẫn đến $MTTF_d$ = 6,7 năm đối với kênh.

Vì cả hai kênh có $MTTF_d$ khác nhau cho nên có thể sử dụng công thức D.2 để tính toán một giá trị thay thế đối với $MTTF_d$ một kênh của hệ thống hai kênh đối xứng. Công thức này dẫn đến $MTTF_d$ = 20 năm hoặc "trung bình" đối với kênh theo 4.5.2, Bảng 5.

- **DC**

Trong mạch điều khiển B, bốn bộ phận liên quan đến an toàn được thử nghiệm bởi PLC: SW2 và K1B được đọc lùi bởi PLC, PLC thực hiện các phép tự thử nghiệm và CC được đọc lùi qua NC bởi PLC. DC có liên quan của mỗi bộ phận được thử nghiệm là

1) DC_{SW2} = 60 %, "thấp", do sự giám sát các tín hiệu nhập không qua thử nghiệm động lực học, xem Bảng E.1 (hàng thứ ba của phần thiết bị nhập),

2) DC_{K1B} = 99 %, "cao", do các tiếp điểm thường mở và thường đóng được liên kết cơ khí, xem Bảng E.1 (hàng thứ hai của phần thiết bị nhập),

3) DC_{PLC} = 30 %, "không", do hiệu quả thấp của các phép tự thử nghiệm (giả thiết rằng nhà sản xuất đã tính toán giá trị này bằng FMEA) và

4) DC_{CC} = 90 %, "trung bình", do đường dẫn ngắt dư thừa có sự giám sát cơ cấu chấp hành (tác động) bằng hệ thống logic điều khiển, xem Bảng E.1 (hàng thứ sáu của phần thiết bị xuất) - nếu PLC giám sát một hư hỏng của CC thì có thể dừng chuyển động với việc tạo khối xung an toàn (đường dẫn ngắt bổ sung).

Để dự tính PL, cần có một giá trị trung bình của DC (DC_{avg}) với tư cách là dữ liệu nhập đối với Hình 5.

$$DC_{avg} = \frac{\frac{DC_{SW2}}{\mathrm{MTTF}_{d\,SW2}} + \frac{DC_{K1B}}{MTTF_{dK1B}} + \frac{DC_{PLC}}{MTTF_{dPLC}} + \frac{DC_{CC}}{MTTF_{dCC}}}{\frac{1}{MTTF_{dSW2}} + \frac{1}{MTTF_{dK1B}} + \frac{1}{MTTF_{dPLC}} + \frac{1}{MTTF_{dCC}}}$$

$$= \frac{\frac{0,6}{20năm} + \frac{0,99}{30năm} + \frac{0,3}{20năm} + \frac{0,9}{20năm}}{\frac{1}{20năm} + \frac{1}{30năm} + \frac{1}{20năm} + \frac{1}{20năm}} = \frac{0,123}{0,183} = 67,1\% \qquad (I.4)$$

Như vậy là "thấp" theo 4.5.3 và Bảng 6.

– CCF

Sự dự tính các biện pháp tránh CCF theo F.2 được giả thiết là đã được thực hiện đối với mạch điều khiển B. Điểm số được yêu cầu như đã cho trong Bảng I.1.

Bảng I.1 - Dự tính các biện pháp phòng tránh CCF đối với ví dụ B

TT	Biện pháp phòng tránh CCF	Điểm cho mạch điều khiển	Điểm tối đa có thể đạt
1	Tách biệt/tách rời		
	Tách biệt về vật lý giữa các đường dẫn tín hiệu	15	15
2	Tính đa dạng		
	Các công nghệ/thiết kế khác nhau hoặc các nguyên tắc vật lý được sử dụng	20	20
3	Thiết kế/ứng dụng/kinh nghiệm		
3.1	Bảo vệ tránh quá điện áp, quá áp suất, quá dòng điện v.v...	Không	15
3.2	Các bộ phận (linh kiện) được sử dụng là đã quen - đáng tin cậy	5	5
4	Đánh giá/phân tích		
	Các kết quả của một dạng hư hỏng và phân tích ảnh hưởng có được tính đến hay chưa để tránh hư hỏng do nguyên nhân chung trong thiết kế	5	5
5	Kỹ năng/huấn luyện		
	Người thiết kế đã được huấn luyện để hiểu được các nguyên nhân và hậu quả của các hư hỏng do nguyên nhân chung hay chưa ?	Không	5
6	Môi trường		
6.1	Sự phòng ngừa nhiễm bẩn và tính tương thích điện từ (EMC) tránh CCF theo các tiêu chuẩn thích hợp	25	25
6.2	Các ảnh hưởng khác Các yêu cầu về tính miễn dịch đối với tất cả các ảnh hưởng của môi trường có liên quan như nhiệt độ, va chạm, rung, độ ẩm, (ví dụ, như đã quy định trong các tiêu chuẩn có liên quan) đã được xem xét chưa?		
	Tổng	80	100 Max

Các biện pháp thích hợp phòng tránh CCF yêu cầu một số điểm tối thiểu là 65. Trong ví dụ B, số điểm 80 là đủ để đáp ứng các yêu cầu phòng tránh CCF.

Một lỗi trong bất cứ bộ phận nào cũng không dẫn đến làm mất đi chức năng an toàn. Khi có thể thực hiện được lỗi đơn nên được phát hiện tại lúc hoặc trước lúc có yêu cầu tiếp theo đối với chức năng an toàn. Vùng chẩn đoán (DC_{avg}) nằm trong phạm vi 60 % đến 90 %. Các biện pháp phòng tránh CCF là đầy đủ. Đây là các đặc tính điển hình đối với loại 3.

Các dữ liệu nhập đối với Hình 5: $MTTF_d$ đối với kênh là "trung bình" (20 năm), DC_{avg} là "thấp" và loại là loại 3.

Kết quả này có thể được giải thích như mức tính năng c.

Kết quả này phù hợp với mức tính năng yêu cầu c của I.2. Như vậy mạch kiểm tra B đáp ứng các yêu cầu về giảm rủi ro của ví dụ trong I.2.

Phụ lục J

(Tham khảo)

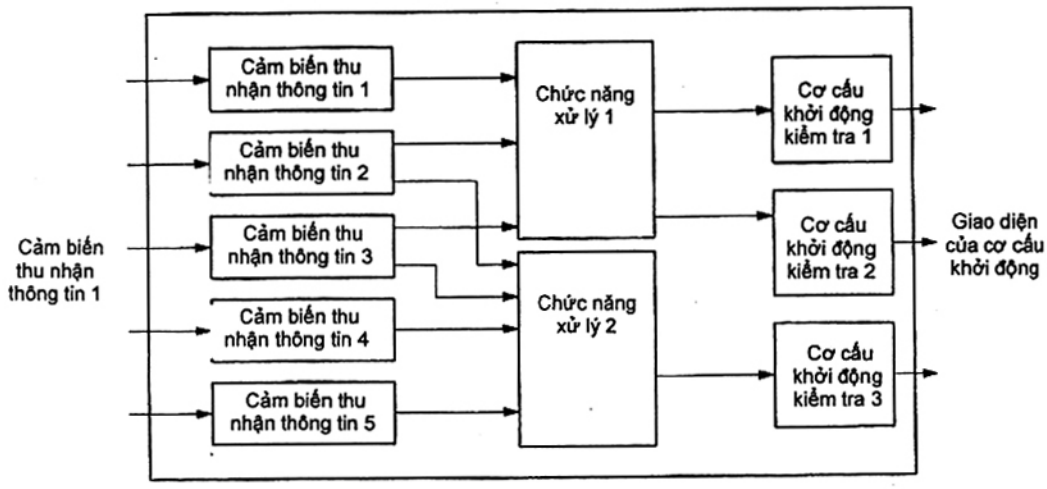
Phần mềm

J.1 Mô tả ví dụ

Trong Phụ lục này giới thiệu hoạt động tiêu biểu để thực hiện phần mềm được nhúng liên quan đến an toàn (SRESW) của một bộ phận liên quan đến an toàn của hệ thống điều khiển (SRP/CS). SRP/CS được tiếp xúc với thiết bị của máy. Nó đảm bảo

- Thu nhận thông tin gửi đến từ các cảm biến khác nhau,
- Xử lý thông tin theo yêu cầu để vận hành các bộ phận điều khiển có tính đến các yêu cầu an toàn, và
- Điều khiển các cơ cấu chấp hành (khởi động).

Việc thiết kế SRESW của ứng dụng này ở mức sơ đồ khối chức năng được giới thiệu trên Hình J.1.



Hình J.1 – Thiết kế sơ đồ khối chức năng của ví dụ về phần mềm

J.2 Ứng dụng mẫu V của vòng đời an toàn của phần mềm

Bảng J.1 giới thiệu tổng hợp các hoạt động tiêu biểu và các tài liệu về ứng dụng mẫu V của vòng đời an toàn của phần mềm cho điều khiển máy.

Bảng J.1 – Các hoạt động và tài liệu trong vòng đời an toàn của phần mềm

Hoạt động triển khai	Hoạt động kiểm tra	Tài liệu gắn liền
Về máy: Nhận biết các chức năng liên quan đến SRP/CS	Nhận biết các chức năng liên quan đến an toàn	"Đặc tả liên quan đến an toàn cho điều khiển máy"
Về cấu trúc: Xác định cấu trúc điều khiển có các cảm biến và cơ cấu khởi động	Dẫn giải về các đặc tính an toàn của các thành phần được lựa chọn	"Xác định cấu trúc điều khiển"
Về đặc tả phần mềm: Chuyển dịch các chức năng của máy thành các chức năng của phần mềm	Đọc lại các mô tả (xem J.3)	"Mô tả phần mềm"
Về cấu trúc phần mềm" Chi tiết hoá các chức năng thành các khối chức năng	Xác định các khối tới hạn cần được xem xét một cách thích hợp và làm cho có hiệu lực	"Lập mô hình khối chức năng"
Về mã hoá: Mã hoá theo các quy tắc lập trình (xem J.4)	Đọc lại mã. Kiểm tra các chức năng và sự tuân theo các quy tắc	"Mã hoá các dẫn giải trong mã" "Mã hoá các tấm giấy đọc lại"
Về việc làm cho có hiệu lực: Thực hiện các kịch bản thử nghiệm về Vận hành các chức năng Trạng thái của hư hỏng	Kiểm tra sai số thử nghiệm Kiểm tra các kết quả thử	"Ma trận tương ứng" tham chiếu các đoạn văn bản đặc tả và các thử nghiệm "Các tấm giấy thử nghiệm" gồm kịch bản thử nghiệm và dẫn giải về các kết quả đạt được

J.3 Kiểm tra đặc tả của phần mềm

Là một phần của vòng đời an toàn của phần mềm, hoạt động kiểm tra ở mức đặc tả phần mềm chủ yếu là đọc các mô tả để xác minh rằng tất cả các điểm nhạy được mô tả đúng. Nên xem xét các yêu cầu sau khi xác minh mỗi chức năng:

- Hạn chế các trường hợp thông dịch sai đặc tả của hệ thống;
- Tránh các khe trong đặc tả dẫn đến các trạng thái chưa từng được biết của SRP/CS;
- Xác định một cách chính xác các điều kiện để hoạt động và ngừng hoạt động của các chức năng;
- Bảo đảm một cách chính xác rằng tất cả các trường hợp có thể xảy ra đã được xử lý;
- Thử nghiệm tính nhất quán;
- Các trường hợp tham số hoá khác nhau;
- Sự phản ứng theo sau một hư hỏng.

J.4 Ví dụ về các quy tắc lập trình

Đối với CCF, thông thường tác giả nên làm cho chương trình có tính xác thực về thời hạn tải, phiên bản và kiểu truy cập cuối cùng. Về các quy tắc lập trình, có thể cần phải phân biệt các quy tắc sau:

a) Quy tắc lập trình ở mức cấu trúc chương trình

Việc lập trình nên được cấu trúc để hiển thị sườn chung ổn định và có thể hiểu được, cho phép khoanh lại một các dễ dàng các xử lý khác nhau. Yêu cầu này có nghĩa là:

1) Sử dụng các mẫu cho chương trình điển hình hoặc các khối chức năng,
2) Phân chia chương trình thành các đoạn để nhận biết các phần chính tương đương với "các khối nhập", "khối xử lý" và "các khối xuất",
3) Dẫn giải về mỗi phần của chương trình trong nguồn chương trình để dễ dàng cập nhật sự dẫn giải trong trường hợp có cải tiến,
4) Mô tả vai trò của khối chức năng cần phải có khi gọi khối này,
5) Vị trí của bộ nhớ chỉ nên được sử dụng bởi một loại kiểu dữ liệu duy nhất và được đánh dấu bằng các nhãn duy nhất, và
6) Tuần tự làm việc không nên phụ thuộc vào các biến đổi như địa chỉ nhảy được tính toán ở thời gian chạy của chương trình, các bước nhảy có điều kiện được phép.

b) Quy tắc lập trình đối với việc sử dụng biến đổi

- Sự hoạt động hoặc không hoạt động của bất cứ sự xuất hiện nào chỉ nên diễn ra một lần (các điều kiện tập trung).

- Chương trình nên được cấu trúc sao cho các phương trình dùng cho sự cập nhật một biến số được tập trung.
- Mỗi sự biến đổi toàn cục, nhập hoặc xuất, nên có một tên giúp trí nhớ đủ rõ và được mô tả bởi một dẫn giải trong nguồn.

c) Quy tắc lập trình ở một khối chức năng

- Sử dụng ưu tiên các khối chức năng đã được nhà cung cấp SRP/CS làm cho có hiệu lực, kiểm tra bảo đảm cho các điều kiện hoạt động đã giả thiết cho các khối có hiệu lực này tương đương với các điều kiện của chương trình.
- Kích thước của khối được mã hoá nên được hạn chế tới các giá trị hướng dẫn sau:
  i) Các tham số - tối đa là tám dữ liệu số nhập và hai dữ liệu số nguyên nhập, một xuất;
  ii) Mã chức năng - tối đa là miền biến đổi cục bộ, tối đa là 20 phương trình luận lý.
- Các khối chức năng không nên cải tiến các biến đổi toàn cục.
- Một giá trị số nên được điều khiển về chuẩn quy chiếu toàn lập để bảo đảm miền có hiệu lực.
- Một khối chức năng nên cố gắng phát hiện tính không nhất quán của các biến đổi được xử lý.
- Mã lỗi của một khối nên truy cập được để phân biệt một lỗi trong các lỗi khác.
- Các mã lỗi và trạng thái của khối sau khi phát hiện lỗi nên được mô tả bằng các dẫn giải.
- Sự đặt lại khối hoặc sự khôi phục lại trạng thái bình thường nên được mô tả bằng các dẫn giải.

Phụ lục K

(tham khảo)

Biểu thị bằng số của Hình 5

Xem Bảng K.1.

Bảng K.1 – Biểu thị bằng số của Hình 5

	Xác suất trung bình của một hư hỏng nguy hiểm trên giờ (1/h) và mức tính năng (PL) tương ứng															
$MTTF_d$ cho mỗi kênh năm	Loại B PL DC_{avg} = không		Loại 1 PL DC_{avg} = không		Loại 2 PL DC_{avg} = thấp		Loại 2 PL DC_{avg} = trung bình		Loại 3 PL DC_{avg} = thấp		Loại 3 PL DC_{avg} = trung bình		Loại 4 PL DC_{avg} = cao	
3	$3,80 \times 10^{-5}$	a			$2,58 \times 10^{-5}$	a	$1,99 \times 10^{-5}$	a	$1,26 \times 10^{-5}$	a	$6,09 \times 10^{-6}$	b		
3,3	$3,46 \times 10^{-5}$	a			$2,33 \times 10^{-5}$	a	$1,79 \times 10^{-5}$	a	$1,13 \times 10^{-5}$	a	$5,41 \times 10^{-6}$	b		
3,6	$3,17 \times 10^{-5}$	a			$2,13 \times 10^{-5}$	a	$1,62 \times 10^{-5}$	a	$1,03 \times 10^{-5}$	a	$4,86 \times 10^{-6}$	b		
3,9	$2,93 \times 10^{-5}$	a			$1,95 \times 10^{-5}$	a	$1,48 \times 10^{-5}$	a	$9,37 \times 10^{-6}$	b	$4,40 \times 10^{-6}$	b		
4,3	$2,65 \times 10^{-5}$	a			$1,76 \times 10^{-5}$	a	$1,33 \times 10^{-5}$	a	$8,39 \times 10^{-6}$	b	$3,89 \times 10^{-6}$	b		
4,7	$2,43 \times 10^{-5}$	a			$1,60 \times 10^{-5}$	a	$1,20 \times 10^{-5}$	a	$7,58 \times 10^{-6}$	b	$3,48 \times 10^{-6}$	b		
5,1	$2,24 \times 10^{-5}$	a			$1,47 \times 10^{-5}$	a	$1,10 \times 10^{-5}$	a	$6,91 \times 10^{-6}$	b	$3,15 \times 10^{-6}$	b		
5,6	$2,04 \times 10^{-5}$	a			$1,33 \times 10^{-5}$	a	$9,87 \times 10^{-6}$	b	$6,21 \times 10^{-6}$	b	$2,80 \times 10^{-6}$	c		
6,2	$1,84 \times 10^{-5}$	a			$1,19 \times 10^{-5}$	a	$8,80 \times 10^{-6}$	b	$5,53 \times 10^{-6}$	b	$2,47 \times 10^{-6}$	c		
6,8	$1,68 \times 10^{-5}$	a			$1,08 \times 10^{-5}$	a	$7,93 \times 10^{-6}$	b	$4,98 \times 10^{-6}$	b	$2,20 \times 10^{-6}$	c		
7,5	$1,52 \times 10^{-5}$	a			$9,75 \times 10^{-6}$	b	$7,10 \times 10^{-6}$	b	$4,45 \times 10^{-6}$	b	$1,95 \times 10^{-6}$	c		
8,2	$1,39 \times 10^{-5}$	a			$8,87 \times 10^{-6}$	b	$6,43 \times 10^{-6}$	b	$4,02 \times 10^{-6}$	b	$1,74 \times 10^{-6}$	c		
9,1	$1,25 \times 10^{-5}$	a			$7,94 \times 10^{-6}$	b	$5,71 \times 10^{-6}$	b	$3,57 \times 10^{-6}$	b	$1,53 \times 10^{-6}$	c		
10	$1,12 \times 10^{-5}$	a			$7,18 \times 10^{-6}$	b	$5,14 \times 10^{-6}$	b	$3,21 \times 10^{-6}$	b	$1,36 \times 10^{-6}$	c		
11	$1,04 \times 10^{-5}$	a			$6,44 \times 10^{-6}$	b	$4,53 \times 10^{-6}$	b	$2,81 \times 10^{-6}$	c	$1,18 \times 10^{-6}$	c		
12	$9,51 \times 10^{-6}$	b			$5,84 \times 10^{-6}$	b	$4,04 \times 10^{-6}$	b	$2,49 \times 10^{-6}$	c	$1,04 \times 10^{-6}$	c		
13	$8,78 \times 10^{-6}$	b			$5,33 \times 10^{-6}$	b	$3,64 \times 10^{-6}$	b	$2,23 \times 10^{-6}$	c	$9,21 \times 10^{-7}$	d		

Bảng K.1 – Biểu thị bằng số của Hình 5 (kết thúc)

	Xác suất trung bình của một hư hỏng nguy hiểm trên giờ (1/h) và mức tính năng (PL) tương ứng							
$MTTF_d$ cho mỗi kênh năm	Loại B PL DC_{avg} = không	Loại 1 PL DC_{avg} = không	Loại 2 PL DC_{avg} = thấp	Loại 2 PL DC_{avg} = trung bình	Loại 3 PL DC_{avg} = thấp	Loại 3 PL DC_{avg} = trung bình	Loại 4 PL DC_{avg} = cao
15	$7{,}61 \times 10^{-6}$ b		$4{,}53 \times 10^{-6}$ b	$3{,}01 \times 10^{-6}$ b	$1{,}82 \times 10^{-6}$ c	$7{,}44 \times 10^{-7}$ d	
16	$7{,}13 \times 10^{-6}$ b		$4{,}21 \times 10^{-6}$ b	$2{,}77 \times 10^{-6}$ c	$1{,}67 \times 10^{-6}$ c	$6{,}76 \times 10^{-7}$ d	
18	$6{,}34 \times 10^{-6}$ b		$3{,}68 \times 10^{-6}$ b	$2{,}37 \times 10^{-6}$ c	$1{,}41 \times 10^{-6}$ c	$5{,}67 \times 10^{-7}$ d	
20	$5{,}71 \times 10^{-6}$ b		$3{,}26 \times 10^{-6}$ b	$2{,}06 \times 10^{-6}$ c	$1{,}22 \times 10^{-6}$ c	$4{,}85 \times 10^{-7}$ d	
22	$5{,}19 \times 10^{-6}$ b		$2{,}93 \times 10^{-6}$ c	$1{,}82 \times 10^{-6}$ c	$1{,}07 \times 10^{-6}$ c	$4{,}21 \times 10^{-7}$ d	
24	$4{,}76 \times 10^{-6}$ b		$2{,}65 \times 10^{-6}$ c	$1{,}62 \times 10^{-6}$ c	$9{,}47 \times 10^{-7}$ d	$3{,}70 \times 10^{-7}$ d	
27	$4{,}23 \times 10^{-6}$ b		$2{,}32 \times 10^{-6}$ c	$1{,}39 \times 10^{-6}$ c	$8{,}04 \times 10^{-7}$ d	$3{,}10 \times 10^{-7}$ d	
30		$2{,}80 \times 10^{-6}$ b	$2{,}06 \times 10^{-6}$ c	$1{,}21 \times 10^{-6}$ c	$6{,}94 \times 10^{-7}$ d	$2{,}65 \times 10^{-7}$ d	$9{,}[illegible] \times 10^{-8}$ e
33		$3{,}46 \times 10^{-6}$ b	$1{,}85 \times 10^{-6}$ c	$1{,}06 \times 10^{-6}$ c	$5{,}94 \times 10^{-7}$ d	$2{,}30 \times 10^{-7}$ d	$8{,}57 \times 10^{-8}$ e
36		$3{,}17 \times 10^{-6}$ b	$1{,}67 \times 10^{-6}$ c	$9{,}39 \times 10^{-7}$ d	$5{,}16 \times 10^{-7}$ d	$2{,}01 \times 10^{-7}$ d	$7{,}77 \times 10^{-8}$ e
39		$2{,}93 \times 10^{-6}$ c	$1{,}53 \times 10^{-6}$ c	$8{,}40 \times 10^{-7}$ d	$4{,}53 \times 10^{-7}$ d	$1{,}78 \times 10^{-7}$ d	$7{,}11 \times 10^{-8}$ e
43		$2{,}65 \times 10^{-6}$ c	$1{,}37 \times 10^{-6}$ c	$7{,}34 \times 10^{-7}$ d	$3{,}87 \times 10^{-7}$ d	$1{,}54 \times 10^{-7}$ d	$6{,}37 \times 10^{-8}$ e
47		$2{,}43 \times 10^{-6}$ c	$1{,}24 \times 10^{-6}$ c	$6{,}49 \times 10^{-7}$ d	$3{,}35 \times 10^{-7}$ d	$1{,}34 \times 10^{-7}$ d	$5{,}76 \times 10^{-8}$ e
51		$2{,}24 \times 10^{-6}$ c	$1{,}13 \times 10^{-6}$ c	$5{,}80 \times 10^{-7}$ d	$2{,}93 \times 10^{-7}$ d	$1{,}19 \times 10^{-7}$ d	$5{,}26 \times 10^{-8}$ e
56		$2{,}04 \times 10^{-6}$ c	$1{,}02 \times 10^{-6}$ c	$5{,}10 \times 10^{-7}$ d	$2{,}52 \times 10^{-7}$ d	$1{,}03 \times 10^{-7}$ d	$4{,}73 \times 10^{-8}$ e
62		$1{,}84 \times 10^{-6}$ c	$9{,}06 \times 10^{-7}$ d	$4{,}43 \times 10^{-7}$ d	$2{,}13 \times 10^{-7}$ d	$8{,}84 \times 10^{-8}$ e	$4{,}22 \times 10^{-8}$ e
68		$1{,}68 \times 10^{-6}$ c	$8{,}17 \times 10^{-7}$ d	$3{,}90 \times 10^{-7}$ d	$1{,}84 \times 10^{-7}$ d	$7{,}68 \times 10^{-8}$ e	$3{,}80 \times 10^{-8}$ e
75		$1{,}52 \times 10^{-6}$ c	$7{,}31 \times 10^{-7}$ d	$3{,}40 \times 10^{-7}$ d	$1{,}57 \times 10^{-7}$ d	$6{,}62 \times 10^{-8}$ e	$3{,}41 \times 10^{-8}$ e
82		$1{,}39 \times 10^{-6}$ c	$6{,}61 \times 10^{-7}$ d	$3{,}01 \times 10^{-7}$ d	$1{,}35 \times 10^{-7}$ d	$5{,}79 \times 10^{-8}$ e	$3{,}08 \times 10^{-8}$ e
91		$1{,}25 \times 10^{-6}$ c	$5{,}88 \times 10^{-7}$ d	$2{,}61 \times 10^{-7}$ d	$1{,}14 \times 10^{-7}$ d	$4{,}94 \times 10^{-8}$ e	$2{,}74 \times 10^{-8}$ e
100		$1{,}[illegible] \times 10^{-6}$ c	$5{,}[illegible] \times 10^{-7}$ d	$2{,}[illegible] \times 10^{-7}$ d	$1{,}[illegible] \times 10^{-7}$ d	$4{,}[illegible] \times 10^{-8}$ e	$2{,}[illegible] \times 10^{-8}$ e

Thư mục tài liệu tham khảo

Tài liệu xuất bản về các hệ thống điện tử lập trình

[1] IEC 61000–4–4, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 4: Electrical fast transient/burst immunity test* (Tính tương thích điện từ (EMC) – Phần 4: Thử nghiệm và kỹ thuật đo – Đoạn 4: Thử quá trình chuyển tiếp điện nhanh/tính miễn nhiễm đối với xung điện).

[2] IEC 61496–1, *Safety of machinery - Electro–sensitive protective equipment – Part 1: General requirements and tests* (An toàn máy – Thiết bị bảo vệ nhạy cảm điện – Phần 1: Yêu cầu chung và các phép thử).

[3] IEC 61496–2, *Safety of machinery - Electro–sensitive protective equipment – Part 2: Particular requirements for equipment using active opto–electronic protective devices* (An toàn máy – Thiết bị bảo vệ nhạy cảm điện – Phần 2: Yêu cầu cụ thể đối với thiết bị sử dụng các cơ cấu bảo vệ quang điện tử phóng xạ).

[4] IEC 61496–3, *Safety of machinery - Electro–sensitive protective equipment – Part 3: Particular requirements for active opto–electronic protective devices responsive to diffuse reflection (AOPDDR)* (An toàn máy – Thiết bị bảo vệ nhạy cảm điện – Phần 3: Yêu cầu cụ thể đối với thiết bị bảo vệ quang điện tử phóng xạ đối với sự phản xạ khuyếch tán).

[5] IEC 61508–1 : 1998, *Functional safety of electrical/electronic/programmable electronic safety–related systems – Part 1: General requirements* (An toàn chức năng của các hệ thống liên quan đến an toàn điện/điện tử/điện tử lập trình – Phần 1: Yêu cầu chung).

[6] IEC 61508–2:2000, *Functional safety of electrical/electronic/programmable electronic safety–related systems – Part 2: Requirement for electrical/electronic/programmable electronic safety-related systems* (An toàn chức năng của các hệ thống liên quan đến an toàn điện/điện tử/điện tử lập trình – Phần 2: Yêu cầu đối với hệ thống liên quan đến an toàn điện/điện tử/điện tử lập trình.

[7] IEC 61508–5:1998, *Functional safety of electrical/electronic/programmable electronic safety–related systems - Part 5: Examples of methods for the determination of safety integrity levels* (An toàn chức năng của các hệ thống liên quan đến an toàn điện/điện tử/điện tử lập trình – Phần 5: Ví dụ về các phương pháp xác định mức toàn vẹn của an toàn.

[8] IEC 61508–6:2000, *Functional safety of electrical/electronic/programmable electronic safety–related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3* (An

toàn chức năng của các hệ thống liên quan đến an toàn điện/điện tử/điện tử lập trình – Phần 6: Hướng dẫn về áp dụng IEC 61508-2 và IEC 61508-3.

[9] IEC 61508–7:2000, *Functional safety of electrical/electronic/programmable electronic safety–related systems – Part 7: Overview of techniques and measures* (An toàn chức năng của các hệ thống liên quan đến an toàn điện/điện tử/điện tử lập trình – Phần 7: Mô tả tóm tắt các kỹ thuật và phương pháp.

[10] IEC 62061, *Safety of machinery - Functional safety of safety–related electrical, electronic and peogrammable electronic control systems* (An toàn máy – Chức năng an toàn của hệ thống điều khiển liên quan đến an toàn điện, điện tử và điện tử lập trình).

[11] HSE Guidelines, *Programmable Electronic Systems in Safety–related Applications*, Parts 1 (ISBN 0 11 883906 6) and 2 (ISBN 0 11 883906 3) (Hướng dẫn – Hệ thống điện tử lập trình trong các ứng dụng liên quan đến an toàn, Phần 1 (ISBN 0 11 883906 6) and 2 (ISBN 0 11 883906 3).

[12] CECR–184, *Personal Safety in Microprocessor Control Systems* (Elektronikcentralen, Denmark) (An toàn của cá nhân trong các hệ thống điều khiển vi xử lý).

Các tài liệu xuất bản khác

[13] TCVN 6719 (ISO/FDIS 13850), An toàn máy – Dừng khẩn cấp – Nguyên tắc thiết kế.

[14] TCVN 7385 (ISO 13851), An toàn máy – Cơ cấu điều khiển hai tay – Chức năng và nguyên tắc thiết kế

[15] ISO 13856–1, *Safety of machinery – Pressure–sensitive protective devices – Part 1: General principles for design and testing of pressure–sensitive mats and pressure–sensitive floors* (An toàn máy – Thiết bị bảo vệ nhạy cảm áp suất – Phần 1: Nguyên tắc chung về thiết kế và thử nghiệm các tấm thảm nhạy cảm áp suất và sàn nhà nhạy cảm áp suất).

[16] ISO 13856–2, *Safety of machinery – Pressure–sensitive protective devices – Part 2: General principles for the design and testing of pressure–sensitive edges and pressure–sensitive bars* (An toàn máy – Thiết bị bảo vệ nhạy cảm áp suất – Phần 2: Nguyên tắc chung về thiết kế và thử nghiệm các tấm thảm nhạy cảm áp suất và các thanh nhạy cảm áp suất).

[17] ISO 11428, *Safety of machinery – Visual danger signals – General requirements, design and testing* (An toàn máy – Tín hiệu nhìn thấy về mối nguy hiểm – Yêu cầu chung, thiết kế và thử nghiệm).

18] TCVN ISO 9001, Hệ thống quản lý chất lượng – Các yêu cầu.

[19] ISO 9355–1, *Ergonomic requirements for the design of displays and control actuators – Part 1: Human interactions with displays and control actuators* (Yêu cầu về êgônômi cho thiết kế các chỉ báo và các cơ cấu dẫn động điều khiển – Phần 1: Giao diện của người với các chỉ báo và cơ cấu dẫn động điều khiển).

[20] ISO 9355–2, *Ergonomic requirements for the design of displays and control actuators – Part 2: Displays* (Yêu cầu về êgônômi cho thiết kế các chỉ báo và các cơ cấu dẫn động điều khiển – Phần 2: Các chỉ báo).

[21] ISO 9355–3, *Ergonomic requirements for the design of displays and control actuators – Part 3: Control actuators Displays* (Yêu cầu về êgônômi cho thiết kế các chỉ báo về các cơ cấu dẫn động điều khiển – Phần 3: Các cơ cấu dẫn động điều khiển).

[22] ISO 11429, *Ergonomic – System of auditory and visual danger and information signals* (Êgônômi – Hệ thống các tín hiệu nghe và nhìn về mối nguy hiểm và tín hiệu thông tin).

[23] ISO 7731, *Ergonomic – Danger signal for public and work areas – Auditory danger signals* (Êgônômi – Tín hiệu về mối nguy hiểm cho khu vực công cộng và khu vực làm việc).

[24] ISO 4413, *Hydraulic fluid power – General rules relating to systems* (Truyền động thủy lực – Các qui tắc chung liên quan đến các hệ thống).

[25] ISO 4414, *Pneumatic fluid power – General rules relating to systems* (Truyền động khí nén – Các qui tắc chung liên quan đến các hệ thống).

[26] TCVN 7386 (ISO 13855), An toàn máy – Định vị thiết bị bảo vệ đối với vận tốc tiếp cận của các bộ phận cơ thể người.

[27] TCVN 7300 (ISO 14118), An toàn máy – Ngăn chặn khởi động bất ngờ.

[28] ISO 19973 (all parts), *Pneumatic fluid power – Assessment of component reliability testing* (Truyền động khí nén – Đánh giá thử nghiệm độ tin cậy của bộ phận cấu thành).

[29] IEC 60204–1 : 2005, *Safety of machinery –Electrical equipment of machines – Part 1: General requirements* (An toàn máy – Thiết bị điện của máy – Phần 1: Yêu cầu chung).

[30] IEC 60447, *Basic and safety principles for man–machine interface (MMI) – Actuating principles* (Nguyên tắc cơ bản và nguyên tắc an toàn đối với giao diện người-máy-MMI – Nguyên tắc vận hành).

[31] IEC 60529, *Degrees of protection provided by enclosures (IP code) (IEC 60529 : 1998)* [Các cấp bảo vệ được cung cấp bởi các rào chắn (mã IP)].

[32] ISO 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)* (Kỹ thuật phân tích đối với độ tin cậy của hệ thống – Quy trình dùng cho dạng hư hỏng và phân tích hiệu quả).

[33] IEC 60947 (all parts), *Low–voltage switchgear and controlgear* (Cơ cấu đóng ngắt và cơ cấu điều khiển điện hạ áp).

[34] IEC 61000–6–2, *Electromagnetic compatibility (EMC) – Part 6–2: Generic standards – Immunity for industrial environments* (Tính tương thích điện từ - EMC – Phần 6-2: Tiêu chuẩn chung – Tính miễn nhiễm đối với môi trường công nghiệp).

[35] IEC 61800–3, *Adjustable speed electrical power drive system – Part 3: EMC requirements and specific test methods* (Hệ thống dẫn động điện có tốc độ điều chỉnh được – Phần 3: Yêu cầu về tính tương thích điện từ - EMC và các phương pháp thử riêng).

[36] IEC 61810 (all parts), *Electromagnetic elementary relays* (Rơ le điện từ sơ cấp).

[37] IEC 61300 (all parts), *Fibre optic interconnecting devices and passive components – Basic test and measurement procedures* (Thiết bị liên kết dùng sợi quang và các thành phần thụ động – Phép thử cơ bản và quy trình đo).

[38] IEC 61310 (all parts), *Safety of machinery – Indication, marking and actuation* (An toàn máy – Chỉ báo, ghi nhãn và khởi động).

[39] IEC 61131–3, *Programmable controllers – Part 3: Programming languages* (Bộ điều khiển lập trình được – Phần 3: Các ngôn ngữ lập trình).

[40] EN 455, *Safety of machinery - Auditory danger signals - General requirements, design and testing* (An toàn máy - Tín hiệu nguy hiểm thính giác - Yêu cầu chung, Thiết kế và thử nghiệm)

[41] EN 614-1, *Safety of machinery - Ergonomic danger signals - Part 1: Terminology and general principles* (An toàn máy - Tín hiệu nguy hiểm êgônômi - Phần 1: Thuật ngữ và nguyên lý chung).

[42] EN 982 : 1996, *Safety of machinery – Safety requirements for fluid power systems and their components – Hydraulics* (An toàn máy – Các yêu cầu về an toàn đối với các hệ thống thuỷ lực và khí nén và các bộ phận của chúng – Thiết bị thuỷ lực).

[43] EN 983 : 1996, *Safety of machinery – Safety requirements for fluid power systems and their components – Pneumatics* (An toàn máy – Các yêu cầu về an toàn đối với các hệ thống thuỷ lực và khí nén và các bộ phận của chúng – Thiết bị khí nén).

[44] EN 1005–3, Safety of machinery – Human physical performance – Part 3: Recommended force limits for machinery operation (An toàn máy – Đặc tính vật lý của con người – Phần 3: Các giới hạn về lực nên dùng cho vận hành máy).

[45] *EN 1088 : 1995 (ISO 14119 : 1998), Safety of machinery – Interlocking devices associated with guards – Principles for design and selection* (An toàn máy – Các cơ cấu khoá liên động liên kết với các thiết bị bảo vệ – Các nguyên tắc để thiết kế và lựa chọn).

[46] EN 50205 : 2002 *Relays with forcibly guided (mechanically linked) contacts* [Rơ le có các tiếp điểm được dẫn hướng cưỡng bức (liên kết cơ khí)].

[47] NS 29500 (all parts), Failure rates of components (Tốc độ hư hỏng của các bộ phận).

[48] GOBLE, W.M, *Control systems – Evaluation and Rehability*. 2nd Edition. Instrument society of America (ISA), North Carolina, 1998

Cơ sở dữ liệu

[49] NS 29500, *Failure rates of components*, Edition 1999–11, siemens AG 1999, www.pruefinstitut.de

[50] IEC/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment, identical to RDF 2000/Reliability Data Handbook*, UTE C 80–810, Union Technique de l'Electricité et la Communication (www.ute–fr.com)

[51] *Reliability Prediction of Electronic Equipment*, MIL–HDBK–217E, Department of Defense, Washington DC, 1982

[52] *Reliability Prediction Procedure for Electronic Equipment*, Telcordia SR–332, Issue 01, May 2001 (telecom–info.telcordia.com), Bellcore TR–332, Issue 06

[53] EPRD, *Electronic Parts Reliability* Data (RAC–STD–6100), Reliability Analysis Centre, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com)

[54] NPRD–95, Non–electronic Parts Reliability Data (RAC–STD–6200), Reliability Analysis Centre, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com)

[55] *British handbook for Reliability Data for Components used in Telecommunication* Systems, British Telecom (HRD5, last issue)

[56] Chinese Military Standard, GJB/z 299B