TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 14447-1:2025

ISO 22166-1:2021

Xuất bản lần 1

RÔ BỐT – HỆ MÔ ĐUN CHO RÔ BỐT DỊCH VỤ – PHẦN 1: YÊU CẦU CHUNG

Robotics – Modularity for service robots – Part 1: General requirements

HÀ NỘI – 2025

Mục lục

Lời nói đầu

TCVN 14447-1:2025 hoàn toàn tương đương với ISO 22166-1:2021.

TCVN 14447-1:2025 do Ban kỹ thuật tiêu chuẩn quốc gia TCVN/TC 299 *Robot* biên soạn, Viện Tiêu chuẩn Chất lượng Việt Nam đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Rô bốt –

Hệ mô đun cho rô bốt dịch vụ – Phần 1: Yêu cầu chung

Robotics –

Modularity for service robots – Part 1: General requirements

1 Phạm vi áp dụng

Tiêu chuẩn này giới thiệu các yêu cầu và nguyên tắc đối với thông số kỹ thuật của các nền tảng hệ mô đun, thiết kế mô đun mở và tích hợp các mô đun cho việc triển khai rô bốt phục vụ trong các môi trường khác nhau, bao gồm cả lĩnh vực cá nhân và chuyên nghiệp.

Tiêu chuẩn này dành cho các nhóm người sử dụng sau:

- Các nhà phát triển khung chuẩn cho rô bốt dịch vụ hệ mô đun để xác định các khung chuẩn hiệu quả một cách rõ ràng;
- Các nhà thiết kế hoặc sản xuất mô đun để cung cấp cho người dùng cuối hoặc cho các nhà tích hợp rô bốt;
- Các nhà tích hợp rô bốt dịch vụ để lựa chọn các mô đun có thể áp dụng cho việc xây dựng hệ thống tích hợp.

Tiêu chuẩn này bao gồm các nguyên tắc cho việc áp dụng các tiêu chuẩn hiện hành về an toàn và bảo mật đối với các mô đun rô bốt dịch vụ.

Tiêu chuẩn này không phải là tiêu chuẩn về an toàn.

Tiêu chuẩn này áp dụng đặc biệt cho rô bốt dịch vụ, mặc dù các nguyên tắc về hệ mô đun trong tiêu chuẩn này có thể được sử dụng bởi các nhà phát triển nền tảng, các nhà sản xuất, tích hợp mô đun trong các lĩnh vực khác, không nhất thiết bị giới hạn trong lĩnh vực rô bốt.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây 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 (nếu có).

TCVN 13697 (ISO 9787), Rô bốt và thiết bị rô bốt – Hệ thống tọa độ và chuyển động danh nghĩa.

ISO 12100:2010, *Safety of machinery - General principles for design - Risk assessment and risk reduction (An toàn máy móc - Nguyên tắc chung cho thiết kế - Đánh giá rủi ro và giảm thiểu rủi ro).*

ISO/TR 22100-4, *Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects (An toàn máy móc - Mối quan hệ với ISO 12100 – Phần 4: Hướng dẫn cho các nhà sản xuất máy móc xem xét các khía cạnh liên quan đến an ninh CNTT (an ninh mạng).*

ISO/IEC 27032, *Information technology - Security techniques - Guidelines for cybersecurity (Công nghệ thông tin - Kỹ thuật bảo mật - Hướng dẫn an ninh mạng).*

IEC 61076-1, *Connectors for electronic equipment - Product requirements - Part 1: Generic specification (Đầu nối cho thiết bị điện tử - Yêu cầu sản phẩm - Phần 1: Thông số kỹ thuật chung).*

IEC 61984, *Connectors - Safety requirements and tests (Đầu nối - Yêu cầu và thử nghiệm an toàn).*

IEC/TS 62443-1-1, *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models (Mạng truyền thông công nghiệp - Bảo mật mạng và hệ thống - Phần 1-1: Thuật ngữ, khái niệm và mô hình).*

IEC 62443-2-1, *Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program (Mạng truyền thông công nghiệp - Bảo mật mạng và hệ thống - Phần 2-1: Thiết lập chương trình bảo mật hệ thống điều khiển và tự động hóa công nghiệp).*

IEC 62443-3-3, *Industrial communication networks- Network and system security - Part 3-3: System security requirements and security levels (Mạng truyền thông công nghiệp - Bảo mật mạng và hệ thống - Phần 3-3: Yêu cầu bảo mật hệ thống và mức độ bảo mật).*

NIST SP 800-154, *Guide to data – centric system threat modelling (Hướng dẫn mô hình hóa mối đe dọa hệ thống tập trung vào dữ liệu).*

NIST SP 800-160 vols 1 and 2, *Systems security engineering considerations for a multidisciplinary approach in the engineering of trustworthy secure systems (Các cân nhắc về kỹ thuật bảo mật hệ thống cho phương pháp tiếp cận đa ngành trong kỹ thuật xây dựng các hệ thống an toàn đáng tin cậy).*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa sau:

3.1 Thuật ngữ chung

3.1.1

Lớp trừu tượng hóa (abstraction layer)

Giao diện đến hệ thống, cho phép một số hoặc tất cả các tiềm lực của hệ thống được tiếp cận theo một cách khác và trừu tượng hơn.

Chú thích 1: Lớp trừu tượng hóa cho một mô đun là giống nhau trong trường hợp hệ thống là mô đun.

3.1.2

Đầu nối (connector)

Cơ cấu vật lý cho phép kết nối và ngắt kết nối giữa các bộ phận của hệ thống.

VÍ DỤ: Các liên kết truyền thông, nguồn, cơ khí.

3.1.3

Mặt lắp ghép điện (electrical interface)

Tổ hợp các đầu nối và vật có tính điện để truyền năng lượng, tín hiệu tương tự hoặc tín hiệu số.

3.1.4

Chu trình thực hiện (execution life cycle)

Máy trạng thái hữu hạn (FSM) để xác định tất cả các trạng thái của việc thực hiện một chức năng của bộ phận.

3.1.5

Lỗi (error)

Sự khác nhau giữa giá trị hoặc trạng thái nhận được từ tính toán, quan sát hoặc đo và giá trị hoặc trạng thái đúng, được chỉ định rõ ràng hoặc xác định chính xác từ lý thuyết.

[NGUỒN: IEC 60050-192:2015, 192-03-02]

3.1.6

Hư hỏng (failure)

Mất khả năng thực hiện chức năng dự kiến.

[NGUỒN: IEC 60050-192:2015, 192-03-02]

3.1.7

Sai sót (fault)

Một trạng thái nội bộ dẫn đến không có khả năng thực hiện chức năng theo yêu cầu.

[NGUỒN: IEC 60050-192:2015, 192-04-01]

3.1.8

Chức năng (function)

Mục tiêu xác định hoặc hành động đặc trưng của một hệ thống, thành phần hoặc mô đun.

[NGUỒN: ISO/IEC/IEEE 24765, 3.1206-5-đã thay đổi]

3.1.9

An toàn chức năng (functional safety)

Một phần của an toàn tổng thể liên quan đến thiết bị có kiểm soát (EUC) và hệ thống kiểm soát thiết bị này, phụ thuộc vào sự vận hành chính xác của các hệ thống liên quan đến an toàn điện, điện tử và điện tử khả lập trình (E/E/PE) và các biện pháp giảm thiểu rủi ro khác.

[NGUỒN: IEC 61508-4:2010, 3.1.12]

3.1.10

Lớp trừu tượng hóa phần cứng (hardware abstraction layer, HAL)

Lớp trừu tượng hóa cho một thành phần/ mô đun chứa đặc điểm phần cứng, với lớp trừu tượng hóa cung cấp sự kiểm soát thành phần/ mô đun đó thông qua giao diện phần mềm.

Chú thích 1: Mục đích của HAL thường là để có thể truy cập các hệ thống xử lý mô đun khác nhau thông qua cùng một giao diện phần mềm.

3.1.11

Mô hình thông tin (information model)

Sự trừu tượng hóa và biểu diễn các thực thể trong một môi trường được quản lý, các tính chất, thuộc tính và hoạt động của chúng và cách chúng liên quan đến nhau.

Chú thích 1: Mô hình thông tin không phụ thuộc vào nơi lưu trữ, cách sử dụng phần mềm, giao thức hoặc nền tảng cụ thể nào.

3.1.12

Bảo mật (security)

Sự kết hợp của tính bảo mật, tính toàn vẹn và tính khả dụng.

[NGUỒN: ISO/TR 17522:2015, 3.19]

3.2 Thuật ngữ liên quan đến thành phần

3.2.1

Thành phần (component)

Một phần của thứ gì đó riêng biệt và có khả năng nhận dạng để tạo ra thứ gì đó lớn hơn khi kết hợp với các phần khác.

Chú thích 1: Thành phần có thể là phần cứng hoặc phần mềm. Một thành phần mà chủ yếu là phần mềm (hoặc phần cứng) cũng được coi như một thành phần phần mềm (hoặc tương ứng, như một thành phần phần cứng).

Chú thích 2: Thành phần không cần phải có tính chất đặc biệt nào liên quan đến hệ mô đun.

Chú thích 3: Thành phần và mô đun có thể được sử dụng thay thế lẫn nhau trong các thuật ngữ chung, nhưng để tránh nhầm lẫn thuật ngữ mô đun được dùng để chỉ một thành phần tuân theo các nguyên tắc được trình bày trong tiêu chuẩn này.

Chú thích 4: Một mô đun là một thành phần, nhưng một thành phần không nhất định phải là một mô đun.

3.2.2

Thành phần phần mềm (software component)

Thành phần mà hệ thống xử lý gồm một thuật toán được lập trình bằng máy tính.

3.2.3

Thành phần phần cứng (hardware component)

Thành phần mà hệ thống xử lý gồm các chi tiết vật lý và bất kỳ phần mềm nhúng nào cần thiết cho hoạt động của nó.

3.3 Thuật ngữ liên quan đến mô đun

3.3.1

Khả năng kết hợp (composability)

Khả năng lắp ráp các mô đun, cả về mặt vật lý và logic (không cần phải hiệu chỉnh các mô đun hoặc thực hiện công việc bổ sung về giao diện), bằng cách sử dụng các kết hợp khác nhau để tạo thành các mô đun mới.

Chú thích 1: Trong khi "tích hợp" thường ngụ ý nỗ lực đáng kể, còn "kết hợp" được ngầm hiểu là chỉ cần nỗ lực hạn chế hoặc không cần nỗ lực.

3.3.2

Cấu hình (configuration)

Sự sắp xếp của một mô đun tổng hợp, liên quan đến số lượng và chủng loại các mô đun được sử dụng, các kết nối và thiết lập cho các mô đun đó để đạt được chức năng mong muốn của rô bốt hệ mô đun nói chung.

Chú thích 1: TCVN 13228 (ISO 8373) cũng định nghĩa thuật ngữ cấu hình (của khớp) nhưng đó là khái niệm khác.

Chú thích 2: Thuật ngữ này mô tả kết quả của một quá trình, tức là trạng thái của một cái gì đó. Quá trình tạo ra một trạng thái như vậy được bao hàm trong thuật ngữ *thiết lập cấu hình* (3.3.3).

3.3.3

Thiết lập cấu hình (configuring)

Thiết lập số lượng, chủng loại mô đun, kết nối và cài đặt cho các mô đun đó để đạt được chức năng mong muốn của một rô bốt dịch vụ hệ mô đun nói chung.

3.3.4

Độ chi tiết (granularity)

Mức độ để đánh giá khả năng một mô đun rô bốt có thể được chia nhỏ thành các mô đun riêng biệt.

3.3.5

Đặc điểm phần cứng (hardware aspects)

Thông tin liên quan đến các tính chất và chức năng cần thiết cho một mô đun, kết nối vật lý của nó, và phạm vi cho phép của các tính chất vật lý của môi trường hoạt động.

Chú thích 1: Thông tin về kết nối vật lý bao gồm các tính chất cơ học (vật liệu, hình dáng, tư thế, kích thước, lực/ mô men), điện, điện từ, khí nén và thủy lực.

Chú thích 2: Các tính chất của môi trường hoạt động bao gồm lực, nhiệt độ, độ ẩm, rung động, va chạm cơ học, sự chiếu sáng, nhiễu (âm và điện từ).

3.3.6

Cơ sở hạ tầng (infrastructure)

Cơ sở vật chất và tài nguyên có cấu trúc để hỗ trợ hoạt động của các mô đun và hệ thống.

3.3.7

Mặt lắp ghép (interface)

Ranh giới chung giữa hai hay nhiều mô đun chức năng, được xác định bởi các đặc tính khác nhau liên quan đến chức năng, trao đổi tín hiệu và các đặc tính khác.

[NGUỒN: ISO/IEC/IEEE 24765:2017, 3.2058, định nghĩa 1]

3.3.8

Khả năng tương tác (interoperability)

Khả năng truyền thông, thực hiện chương trình, truyền dữ liệu hoặc năng lượng giữa các mô đun, hoặc sự kết hợp về mặt vật lý và/hoặc logic, theo cách mà người dùng không cần hoặc chỉ cần có một chút kiến thức về các đặc tính riêng biệt của từng mô đun.

3.3.9

Khả năng hoán đổi (Interchangeability)

Thuộc tính của mô đun cho phép nó có thể dùng để thay thế một mô đun khác.

Chú thích 1: Khả năng hoán đổi này có thể liên quan đến các mô đun được chế tạo bởi cùng một nhà sản xuất hoặc từ những nhà sản xuất khác nhau.

3.3.10

Mặt lắp ghép cơ khí (mechanical interface)

Phương tiện vật lý để kết nối với các mô đun khác được dùng để truyền lực và đơn giản hóa việc vận hành mô đun và/hoặc thiết lập cấu trúc cấu hình.

Chú thích 1: Các lực cần truyền bao gồm các lực được kiểm soát cho mục đích dự kiến như một phần của chức năng đã định và các lực không được kiểm soát, cả cố ý (ví dụ: đỡ kết cấu) và không cố ý (ví dụ: giảm chấn).

Chú thích 2: TCVN 13228 (ISO 8373) sử dụng thuật ngữ này cho mặt lắp ghép cơ khí giữa tay máy và khâu tác động cuối. Trong tiêu chuẩn này, thuật ngữ được sử dụng theo nghĩa rộng hơn, bao gồm bất kỳ mặt ghép cơ khí nào giữa các mô đun rô bốt.

3.3.11

Hệ mô đun (modularity)

Tập hợp các đặc tính cho phép các hệ thống có thể chia tách thành các mô đun riêng lẻ và tái tổ hợp.

3.3.12

Mô đun (module)

Thành phần hoặc cụm các thành phần có mặt lắp ghép xác định kèm theo các hồ sơ thuộc tính để tạo điều kiện thuận lợi cho việc thiết kế, tích hợp, tương tác và tái sử dụng.

Chú thích 1: Mô đun có thể có cả các đặc điểm phần cứng và phần mềm. Nó có thể bao gồm các thành phần hoặc các mô đun khác (phần mềm hoặc phần cứng).

Chú thích 2: Điều này không yêu cầu cũng không ngăn cản việc sử dụng phần mềm mã nguồn mở để triển khai một phần hoặc toàn bộ các chức năng của mô đun mở.

Chú thích 3: Mặc dù về mặt khái niệm, mô đun mở trái ngược với mô đun đóng, nhưng trong tiêu chuẩn này nó vẫn được coi là mô đun đóng, tức là trong một hệ thống rô bốt tuân thủ tiêu chuẩn này thì các mô đun khác chỉ nên thực hiện truyền thông với mô đun mở thông qua các mặt lắp ghép mô đun chính thức do nhà sản xuất chỉ định.

Chú thích 4: Mô đun mở không nhất thiết phải là mô đun tổng hợp, và mô đun tổng hợp không nhất thiết phải là mô đun mở.

3.3.13

Gói (package)

Tập hợp tất cả các tệp nhị phân phần mềm, thông tin cấu hình và các tệp hỗ trợ cần thiết cho một mô đun có các đặc điểm phần mềm hoạt động được đúng như thiết kế được.

Chú thích 1: Gói có thể phụ thuộc vào các gói khác.

3.3.14

Đặc tính của mô đun (module property)

Thuộc tính hoặc đặc điểm của một mô đun.

VÍ DỤ: Đặc tính của mô đun cho phần cứng có thể là mô men xoắn của cơ cấu dẫn động. Đặc tính của mô đun cho phần mềm có thể là thời gian đáp ứng một lệnh mới.

3.3.15

Hồ sơ đặc tính của mô đun (module property profile)

Danh mục các giá trị của một tập hợp con các đặc tính của mô đun.

3.3.16

Chất lượng dịch vụ (quality of service)

Mức hiệu năng tối thiểu về dịch vụ của một mô đun đối với các mô đun kết nối với nó để đảm bảo hoạt động tổng thể đúng như dự kiến.

3.3.17

Cấu hình lại (reconfiguration)

Thay đổi cấu hình của một rô bốt hệ mô đun để đạt được sự thay đổi mong muốn về chức năng của rô bốt.

3.3.18

Khả năng tái sử dụng (reusability)

Khả năng áp dụng các mô đun đã được thiết kế và chế tạo trước đó để tạo điều kiện thuận lợi cho việc phát triển các mô đun và hệ thống rô bốt mới để hiện thực hóa các chức năng cần thiết khác.

3.3.19

Mô đun rô bốt (robot module)

Mô đun dự định để sử dụng như một phần của một hệ thống rô bốt hệ mô đun.

Chú thích 1: Không phải tất cả các mô đun được sử dụng trong hệ thống rô bốt hệ mô đun đều phải là các mô đun kiểu rô bốt, nhưng nếu mục đích chính của mô đun là để sử dụng trong hệ thống rô bốt hệ mô đun thì đó là mô đun kiểu rô bốt.

Chú thích 2: Các mô đun rô bốt ví dụ được trình bày trong Phụ lục B có vai trò quan trọng với hệ mô đun của rô bốt dịch vụ.

3.3.20

Tự cấu hình lại (self-reconfiguration)

Thay đổi cấu hình của rô bốt hệ mô đun thông qua một quy trình tự động mà không cần tương tác từ bên ngoài hệ thống/ hệ thống con, ngoại trừ để khởi tạo quy trình, nếu cần.

Chú thích 1: Thông thường, các kết nối cơ và điện cần được cấu hình lại thủ công, còn việc cấu hình lại các đặc điểm phần mềm được tự động hóa.

3.3.21

Đặc điểm phần mềm (software aspects)

Thông tin liên quan đến các đặc tính phần mềm bên ngoài cần thiết cho một mô đun, mặt lắp ghép của nó và chu trình thực hiện chức năng của mô đun đó.

3.4 Thuật ngữ về phân loại mô đun

3.4.1

Mô đun cơ bản (basic module)

Mô đun không thể chia tách thành các mô đun nhỏ hơn.

VÍ DỤ: Các mô đun cơ bản cho rô bốt dịch vụ có thể được định nghĩa như các mô đun đầu vào, mô đun xử lý, mô đun đầu ra hoặc mô đun hỗ trợ cơ sở hạ tầng.

3.4.2

Mô đun tổng hợp (composite module)

Mô đun được xây dựng từ hai hoặc nhiều mô đun.

Chú thích 1: Nhà sản xuất mô đun có thể cung cấp tài liệu về cấu trúc bên trong của mô đun tổng hợp của mình, bao gồm khả năng truy cập vào các mặt lắp ghép nội bộ, hoặc cung cấp các quy trình để thay thế một số mô đun tích hợp. Tuy nhiên, trong mọi trường hợp, mô đun tổng hợp đề cập trong tiêu chuẩn này được coi là mô đun đóng "mô đun hộp đen".

3.4.3

Mô đun phần cứng (hardware module)

Mô đun có các bộ phận thuần vật lý như các bộ phận cơ khí, các mạch điện tử và bất kỳ phần mềm nào, chẳng hạn như chương trình cơ sở, không thể truy cập từ bên ngoài thông qua ghép nối truyền thông.

Chú thích 1: Mô đun phần cứng có các đặc điểm phần cứng. Nó bao gồm các thành phần phần cứng.

VÍ DỤ 1: Một khớp cơ khí không chứa thiết bị điện tử; các đặc điểm phần cứng của nó bao gồm kích thước, các đặc tính động học, các tấm ghép nối ở cả 2 đầu, vật liệu, độ cứng, lực và mô men xoắn cho phép, v.v...

VÍ DỤ 2: Một khớp cơ khí nâng cao, bao gồm một vi điều khiển, phần mềm trên bộ điều khiển và động cơ để điều khiển các đặc tính như độ cứng hoặc giảm chấn; các đặc điểm phần cứng của nó cũng bao gồm các đầu nối để cấp nguồn cho các thiết bị điện tử nhúng và động cơ nhúng, cũng như việc chỉ định giới hạn điện áp và dòng.

3.4.4

Mô đun phần mềm (software module)

Mô đun chỉ gồm các thuật toán được lập trình.

Chú thích 1: Mô đun phần mềm có các đặc điểm phần mềm. Nó bao gồm các thành phần phần mềm.

3.5 Mô tả đặc tính của các mô đun liên quan đến chức năng chính

3.5.1

Mô đun cơ cấu dẫn động (actuator module)

Mô đun dẫn động (actuating module)

Mô đun đầu ra có chức năng chính làm rô bốt di chuyển thực sự hoặc làm thay đổi thế giới xung quanh rô bốt để đáp ứng các hướng dẫn từ các mô đun khác nhằm hoàn thành tác vụ của hệ thống rô bốt.

3.5.2

Mô đun truyền thông (communication module)

Mô đun với giao diện truyền thông dễ dàng tiếp cận cho các phương tiện khác hoặc cung cấp phương tiện kết nối giữa các mô đun.

Chú thích 1: Các kết nối với phương tiện khác có thể thông qua Wi-Fi, mạng di động, Ethernet, v.v...

3.5.3

Mô đun tính toán (computing module)

Mô đun cung cấp tài nguyên máy tính để các mô đun phần mềm sử dụng.

Chú thích 1: Tài nguyên máy tính là phần cứng để chạy phần mềm và có thể bao gồm các mô đun phân tán.

3.5.4

Mô đun cơ sở hạ tầng (infrastructure module)

Mô đun cung cấp tài nguyên và các tiện ích để hỗ trợ hoạt động của các mô đun khác.

Chú thích 1: Ví dụ về các tiện ích được mô đun khác sử dụng bao gồm các khung cơ khí để làm các điểm kết nối vật lý, cố định cáp truyền thông và cáp nguồn.

Chú thích 2: Ví dụ về các tài nguyên được các mô đun khác sử dụng bao gồm bộ nguồn, bộ nhớ và các bộ xử lý, và cầu (hoặc trung tâm) truyền thông giữa các rô bốt liên kết hoặc giữa rô bốt và các máy chủ.

3.5.5

Mô đun cảm biến (sensing module)

Mô đun đầu vào để thu thập dữ liệu về thế giới xung quanh rô bốt hoặc trạng thái của rô bốt để các mô đun khác sử dụng nhằm hỗ trợ hệ thống rô bốt thực hiện tác vụ của mình.

3.5.6

Mô đun giám sát (supervisor module)

Mô đun phần mềm kiểm tra trạng thái của các mô đun khác và có thể kiểm soát quá trình chuyển đổi từ trạng thái này sang trạng thái khác để thực hiện trình tự hoạt động của các mô đun một cách phù hợp.

4 Quy định chung

4.1 Yêu cầu chung

Điều này giới thiệu các khái niệm thiết yếu đằng sau việc sử dụng hệ mô đun trong rô bốt dịch vụ. Nên sử dụng ngôn ngữ SysML (OMG SysML) để mô tả các khái niệm này. Ngôn ngữ này định nghĩa các loại sơ đồ để mô hình hóa các ứng dụng kỹ thuật hệ thống và cũng hỗ trợ đặc tả, phân tích, thiết kế, kiểm

tra và xác nhận. Các nhà sản xuất nên thực hiện các quy trình kiểm tra và xác nhận để đáp ứng các nguyên tắc về hệ mô đun.

4.2 Nguyên tắc chung của hệ mô đun

4.2.1 Yêu cầu chung

Điều này giải thích các nguyên tắc chung mà thiết kế hệ mô đun phải tuân theo. Mặc dù các nguyên tắc này được trình bày một phần dưới dạng khuyến nghị, nhưng nhà thiết kế hệ mô đun phải:

- công bố tất cả các cách tiếp cận hệ mô đun đã được chọn; và
- cung cấp tất cả thông tin cần thiết để các nhà tích hợp sử dụng mô đun.

Các nguyên tắc này có thể áp dụng chung cho các mô đun có đặc điểm phần cứng hoặc phần mềm. Trong điều này, thuật ngữ mô đun, trừ khi có quy định khác, được sử dụng theo nghĩa rộng nhất của nó để chỉ các mô đun cơ bản hoặc mô đun tổng hợp.

4.2.2 Khả năng kết hợp

Các mô đun phải được thiết kế theo cách mà chúng có thể được lắp ráp về mặt vật lý và logic thành các mô đun tổng hợp để thực hiện các hoạt động phức tạp hơn, đồng thời vẫn duy trì các yêu cầu về hoạt động an toàn. Việc tổ hợp phải có thể thực hiện được nhờ thông tin được cung cấp trên các mặt lắp ghép mà không cần thiết phải biết các thông tin về cấu trúc bên trong. Các mô đun có thể được tổ chức thành các ngân hàng dữ liệu hoặc kho kỹ thuật số để tạo thuận lợi cho việc tái sử dụng. Điều này sẽ được thảo luận thêm tại Điều 7.2.2.

4.2.3 Khả năng tích hợp

Các đặc điểm phần cứng và phần mềm của các mô đun phải được thiết kế theo cách mà chúng có thể được tích hợp để tạo thành các hệ thống lớn hơn nhằm thực hiện các dịch vụ hoặc chức năng mục tiêu đã định. Để cho phép liên kết các mô đun theo cách đáng tin cậy, cần thiết kế các mặt lắp ghép phù hợp. Các khía cạnh an toàn của các hệ thống được tạo thành từ các mô đun được thảo luận trong Điều 5.

4.2.4 Khả năng tương tác

Các mô đun phải được thiết kế theo cách mà chúng có thể liên kết để hoạt động với các mô đun khác. Chúng phải dễ kết nối và cho phép chia sẻ nguồn điện và dữ liệu thông qua các đầu nối phù hợp. Để cho phép trao đổi dữ liệu, các giao thức giao diện phải được xác định và triển khai ở các cấp độ phù hợp, như được chỉ định trong Điều 7.

4.2.5 Tính chi tiết

Chức năng của các mô đun phải đạt được ở mức độ chi tiết phù hợp trong một khung chuẩn hệ mô đun: Mô đun cơ bản và mô đun tổng hợp. Ví dụ về các mô đun cơ bản và mô đun tổng hợp được trình bày trong Phụ lục B.

4.2.6 Tính độc lập của nền tảng

Các mô đun phải được thiết kế theo cách mà chúng có thể được thực hiện trên các rô bốt dịch vụ khác nhau hoặc kết hợp với các bộ mô đun khác nhau mà không cần sửa đổi đáng kể. Các mô đun phần mềm phải được tạo theo cách mà chúng có thể chạy trên các nền tảng khác nhau như hệ thống máy tính nhúng, Linux, Windows hoặc hệ điều hành thời gian thực với các sửa đổi tối thiểu. Các mô đun có các đặc điểm phần cứng được sử dụng trong các hệ thống rô bốt dịch vụ khác nhau phải được vận hành trên các nền tảng khác nhau.

4.2.7 Tính mở

Trong tiêu chuẩn này tính mở phải bao gồm các mặt lắp ghép cơ khí và điện cho các mô đun có đặc điểm phần cứng và các giao diện phần mềm giữa các mô đun phải bao gồm những điều sau: một kiến trúc tham chiếu xác định bao gồm các mô đun có đặc điểm phần cứng và phần mềm, thiết kế của chúng cùng các phương pháp đảm bảo an toàn, bảo mật và phương pháp thử.

Việc tái sử dụng các mô đun phải được hỗ trợ bằng cách cung cấp thông tin liên quan cho các nhà tích hợp, chẳng hạn như sự phụ thuộc và tính không tương thích của chúng.

CHÚ THÍCH: *Thông tin có liên quan có thể bao gồm mã nguồn, tài liệu, mô hình thiết kế có sự hỗ trợ của máy tính (CAD), sơ đồ mạch, kinh nghiệm thiết kế, kiến trúc hệ thống, hệ thống phân cấp phần mềm, thông số kỹ thuật giao diện, v.v...*

4.2.8 Khả năng tái sử dụng

Khả năng tái sử dụng là khả năng các mô đun được sử dụng và sử dụng lại trong các nền tảng khác nhau thông qua các giao diện được xác định phù hợp. Giao diện của các mô đun phải được thiết kế theo cách mà các mô đun có thể được tái sử dụng. Các giao diện có liên quan cho phép tái sử dụng có thể bao gồm các giao diện phần mềm, các đầu nối giữa các mô đun và các mặt lắp ghép của các mô đun.

Khi thích hợp, khả năng tái sử dụng phải được hỗ trợ bằng cách quản lý các bản dựng, cấu hình và các tùy chọn cấu hình lại, khả năng nâng cấp và các yêu cầu bảo trì chung của các mô đun.

4.2.9 An toàn

Các mô đun phải được thiết kế để tuân thủ tiêu chuẩn an toàn có liên quan trong tất cả các ứng dụng có liên quan đến an toàn. Ngoài ra, chúng phải được thiết kế để hỗ trợ an toàn tổng thể của hệ thống mô đun. Các nhà sản xuất mô đun phải cung cấp thông tin cần thiết để hỗ trợ các nhà tích hợp trong thiết kế an toàn của hệ thống.

4.2.10 Bảo mật

Các mô đun có đặc điểm phần mềm hoặc giao diện truyền thông phải được thiết kế để ngăn chặn các nỗ lực truy cập bằng các phương pháp hoặc từ các cá nhân trái phép. Ngoài ra, chúng phải được thiết kế để hỗ trợ bảo mật tổng thể của hệ thống hệ mô đun.

4.3 Trừu tượng hóa

Nên sử dụng một lớp trừu tượng hóa để xác định các giao diện chuẩn giữa phần cứng và phần mềm nhằm:

- hỗ trợ khả năng tương tác và khả năng tái sử dụng;
- đơn giản hóa mô phỏng và mô hình hóa;
- thúc đẩy tính độc lập của việc triển khai và tính độc lập với nền tảng.

CHÚ THÍCH 1: Ví dụ, mô đun phần mềm cảm biến hồng ngoại và mô đun phần mềm cảm biến siêu âm có thể được sử dụng cùng nhau để đo khoảng cách từ rô bốt đến một vật thể gần đó. Hai mô đun này có thể đọc giá trị khoảng cách từ cảm biến hồng ngoại và cảm biến siêu âm thông qua trình điều khiển thiết bị tương ứng của chúng. Trong trường hợp này, hai mô đun có thể không tái sử dụng được và không thể tương tác được vì mỗi mô đun sử dụng trình điều khiển thiết bị riêng, mặc dù cùng một dữ liệu được sử dụng. Để đảm bảo khả năng tái sử dụng của hai mô đun để đọc giá trị khoảng cách, cần một trình điều khiển thiết bị trừu tượng, sau đó một mô đun cảm biến khác có thể được sử dụng nhờ vào lớp trừu tượng hóa, mặc dù nhiều nhà sản xuất cung cấp các loại cảm biến đo khoảng cách khác nhau.

CHÚ THÍCH 2: Các đặc điểm phần mềm trong các mô đun phần mềm sử dụng lớp trừu tượng hóa để truy cập các thiết bị phần cứng như động cơ servo và cảm biến laser.

CHÚ THÍCH 3: Việc sử dụng lớp trừu tượng hóa phần cứng hoặc một dạng trình điều khiển thiết bị khác là tùy chọn trong tiêu chuẩn này (xem 7.3). Nếu có thể đạt được một triển khai cụ thể của hệ thống rô bốt hệ mô đun bằng cách gọi trực tiếp các hàm phần mềm của trình điều khiển thiết bị, thì điều này được phép. Sự trừu tượng hóa có thể bao gồm việc sử dụng các kỹ thuật biên dịch khi các công nghệ truyền thông cơ bản khác nhau.

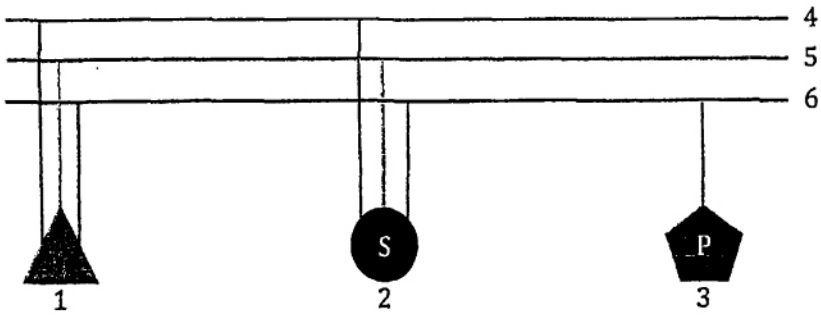
4.4 Mặt lắp ghép điện và giao thức truyền thông

Mặt lắp ghép điện và giao thức truyền thông phải tuân theo các tiêu chuẩn hiện hành.

CHÚ THÍCH 1: Mặt lắp ghép cho bus dữ liệu và mạng truyền thông bao gồm các đặc điểm phần cứng và phần mềm. Một ví dụ có tính khái niệm về cách bố trí mặt lắp ghép tổng quát được thể hiện trên Hình 1 bao gồm chức năng, cấp nguồn và môi trường hoạt động.

CHÚ THÍCH 2: Bảng 1 trình bày một số ví dụ về giao thức truyền thông. Giao thức truyền thông thường được cấy ghép trong phần mềm, nhưng đôi khi cũng được tích hợp trong phần cứng. Chúng đại diện cho lớp 2 đến lớp 7 trong mô hình tham chiếu OSI như được định nghĩa tại TCVN 9696-1 (ISO/IEC 7498-1).

Phần cứng mặt lắp ghép điện phải được thiết kế sao cho thông tin liên lạc không bị nhiễu do gần các dây điện hoặc thiết bị điện khác. Chỉ được sử dụng các đầu ghép nối đã được chuẩn hóa.



CHÚ DẪN:

1 bộ truyền động
2 cảm biến
3 nguồn điện
4 môi trường
5 chức năng
6 nguồn điện

Hình 1 – Ví dụ về cách bố trí mặt lắp ghép giữa các mô đun

(được trình bày chi tiết trong Điều 6)

Bảng 1 – Các ví dụ về giao thức truyền thông cho phép sử dụng giữa các mô đun

Tham chiếu	Loại	Ghi chú
ISO 11898-1/2 Và EN 50325-4/5	CAN và CANopen	Lớp con đơn vị truy cập phương tiện CAN thường được triển khai trong IC thu phát, giao thức lớp liên kết dữ liệu CAN và lớp con tín hiệu vật lý được triển khai trong bộ điều khiển giao thức CAN, và lớp ứng dụng CANopen thường được triển khai trong phần mềm chạy trên bộ vi điều khiển.
ISO/IEC/IEEE 8802-3:2017 IETF 793 or ISO/IEC 14766 (TCP), IETF RFC 768 (UDP), RFC 791 (IPv4), RFC 2460 (IPv6)	Ethernet and TCP/IP	Được triển khai trong PHY và MAC, được tích hợp tùy chọn trong các bộ điều khiển công nghệ cụ thể. (Giao thức này được sử dụng rộng rãi trên toàn thế giới).
IEC 62680 and USB CDC	USB	Có nhiều cách triển khai và lớp thiết bị truyền thông USB (CDC) là lớp thiết bị Universal Serial Bus tổng hợp.
IEC 61158	Fieldbus	IEC 61158 chuẩn hóa các giao thức Fieldbus thường sử dụng và bao gồm Foundation fieldbus, Profibus, WorldFIP, CC-link, EtherCAT Modbus-RTPS, SERCOS, v.v.

4.5 Khả năng hoán đổi

Khả năng hoán đổi và tái tổ hợp các mô đun có liên quan chặt chẽ đến khả năng kết nối của các mô đun và có thể có các cấp độ khác nhau; tiêu chuẩn này xem xét các cấp độ sau:

- Cấp độ 1: Chỉ nhà sản xuất hoặc nhà tích hợp hệ thống rô bốt mới có thể hoán đổi các mô đun.
- Cấp độ 2: Người dùng có thể hoán đổi các mô đun khi rô bốt đã tắt.
- Cấp độ 3: Người dùng có thể hoán đổi các mô đun khi rô bốt đã bật (cắm nóng).

- Cấp độ 4: Rô bốt tự nó có thể hoán đổi các mô đun (cắm nóng với các bộ điều khiển đã kích hoạt).

Tự cấu hình (cấp độ 3 và 4) có thể dẫn đến hoạt động không chính xác hoặc các tình huống nguy hiểm. Các vấn đề về an toàn và bảo mật liên quan được thảo luận trong Điều 5. Để tránh sự mơ hồ về trạng thái của các mô đun, không nên tự cấu hình với các chức năng rô bốt đang diễn ra.

Các nhà sản xuất mô đun phải cung cấp cấp độ hoán đổi cho các mô đun. Các cấp độ khác nhau có ý nghĩa khác nhau đối với các yêu cầu liên quan đến thiết kế đầu nối, an toàn và bảo mật, độ bền, tài liệu về các mô đun, v.v..., như thể hiện trong Bảng 2.

Bảng 2 – Khuyến nghị về các mức độ khác nhau của khả năng hoán đổi

Cấp độ	Tần suất thay đổi	Thiết kế các đầu nối	Tài liệu	An toàn	Phần mềm
1	Thấp	Có thể đơn giản hóa bằng cách kết nối riêng biệt các bộ phận cơ khí và điện.	Dành cho người có kiến thức kỹ thuật.	Các vấn đề cần được đề cập trong đánh giá rủi ro được thực hiện sau khi trao đổi.	Việc cài đặt và cấu hình có thể phức tạp và bao gồm cả việc điều chỉnh thủ công.
2	Trung bình - cao	Tốt nhất là phích cắm composite.	Dành cho người thiếu kiến thức kỹ thuật.	Giới hạn an toàn cần được cung cấp cho người dùng. Hệ thống có thể thực hiện kiểm tra tính nhất quán khi bật nguồn.	Tổ chức theo gói, giải quyết tự động các phụ thuộc.
3	Cao	Phích cắm composite có chức năng cắm nóng.	Dành cho người thiếu kiến thức kỹ thuật.	Giới hạn an toàn cần được cung cấp cho người dùng. hệ thống cần thực hiện kiểm tra tính nhất quán trong khi các chức năng khác được thực thi.	Tự động tải, dỡ và chuyển đổi các mô đun trong thời gian chạy.
4	Cao	Phích cắm composite có chức năng cắm nóng và dung sai lớn cho kết nối tự động.	Dành cho người thiếu kiến thức kỹ thuật.	Giới hạn an toàn cần được cung cấp dưới dạng máy có thể đọc được. hệ thống cần thực hiện kiểm tra tính nhất quán trong khi các chức năng khác được thực thi.	Tự động tải, dỡ và chuyển đổi các mô đun trong thời gian chạy.

4.6 Đặc tính của mô đun

4.6.1 Yêu cầu chung

Các đặc tính của mô đun sẽ được lưu giữ trong hồ sơ đặc tính của mô đun. Khi một mô đun được chuyển giao để sử dụng hoặc tái sử dụng, hồ sơ mô đun sẽ đi kèm với mô đun đó.

CHÚ THÍCH 1: Không có sự ám chỉ nào về bản chất của sự lưu giữ này.

4.6.2 Nhận dạng mô đun

Mô đun phải được đặt tên hoặc nhận dạng bằng mã kiểu chuỗi ký tự hoặc số do nhà sản xuất công bố. Ngoài ra, bản thân sản phẩm và nhà cung cấp cũng phải được xác định bằng tên hoặc mã nhận dạng tương tự. Thông tin này có thể được sử dụng để thiết kế rô bốt dịch vụ dựa trên các mô đun có thể thiết lập cấu hình cho hệ thống rô bốt một cách tự động hoặc bán tự động. Nếu mô đun sử dụng bus dữ liệu, nó phải chuyển mã nhận dạng (ID) của bản thân đến các mô đun khác và đến mô đun giám sát khi được yêu cầu.

Mô đun có thể cung cấp cấu hình tự động của phần cứng (bao gồm cả cấu trúc) và phần mềm của rô bốt.

Nếu tính năng tự động thiết lập cấu hình có sẵn trong mô đun, thông tin tối thiểu được nhà sản xuất cung cấp để nhận dạng mô đun phải là:

- Loại mô đun và/hoặc mã nhận dạng mô đun
- Tên và/hoặc mã nhận dạng nhà sản xuất
- Phiên bản mô đun
- Ngày sản xuất
- Số sê-ri

Theo quan điểm bảo mật hệ thống, việc nhận dạng mô đun đối với các mô đun liên quan đến bảo mật phải được xác minh bằng một quy trình xác thực được thiết kế phù hợp.

4.7 Mô phỏng

Nếu mô phỏng được sử dụng để xác minh thiết kế và chức năng của một mô đun, thì cần phải nhận ra các hạn chế và ràng buộc của các mô hình được sử dụng. Đặc biệt, cần phải xác minh tính an toàn và bảo mật của ứng dụng trong các thử nghiệm thực tế cho việc sử dụng dự kiến.

Để cho phép mô phỏng chính xác một hệ thống hệ mô đun, các nhà sản xuất mô đun phải cung cấp thông tin liên quan cần thiết cho mô phỏng với các mô đun của họ. Nhà thiết kế khung chuẩn phải chỉ định thông tin nào là cần thiết và chúng phải được cung cấp dưới dạng nào (ví dụ: trên giấy hoặc dưới dạng tệp tham số có thể được nhập vào công cụ mô phỏng). Thông tin về mô đun được sử dụng trong mô phỏng có thể bao gồm:

- Các đặc điểm vật lý của mô đun, bao gồm các tính chất vật lý (ví dụ: kích thước, khối lượng, mật độ, đặc điểm tĩnh và động, độ bền cấu trúc, v.v...) và hình thức;
- Các đặc điểm điện của mô đun, chẳng hạn như yêu cầu công suất cực đại và trung bình để vận hành;
- Các thuật toán điều khiển chung mà mô đun có thể thực hiện;

- Các mặt lắp ghép cho các mô đun đầu vào (cảm biến) hoặc mô đun đầu ra (dẫn động), xác định định dạng và kiểu của thông tin cần trao đổi;
- Phương pháp mà mô đun cảm biến thu thập thông tin từ thế giới mô phỏng;
- Phương pháp mà mô đun dẫn động tác động lên thế giới mô phỏng.

CHÚ THÍCH 1: Thông số kỹ thuật chi tiết cho các mô hình khác nhau nằm ngoài phạm vi của tiêu chuẩn này.

CHÚ THÍCH 2: Cũng có thể cung cấp dữ liệu mô phỏng bên trong mẫu mô đun.

4.8 Kiểu dữ liệu cho khả năng tương tác

Khung chuẩn hệ mô đun phải định nghĩa các kiểu dữ liệu có thể được sử dụng trong khung chuẩn hệ mô đun và phần trung gian. Điều này bao gồm độ chính xác của các kiểu dữ liệu số nguyên và số thực phổ biến như trong IEC/TR 62390.

Khung chuẩn hệ mô đun cũng phải định nghĩa các quy ước cho các kiểu dữ liệu tổng hợp thường được sử dụng. Định nghĩa các quy ước sau đây được khuyến nghị. Ngoài ra còn có một số ít kiểu dữ liệu tổng hợp phổ biến được xây dựng dựa trên các kiểu này [xem thêm OMG RLS (Dịch vụ định vị rô bốt)], cụ thể là:

a) Vị trí trong không gian được xác định theo một hệ tọa độ nào đó, được xác định theo một vị trí và hướng cố định phù hợp với việc triển khai. Một tọa độ có thể được cho dưới dạng Đề các trong hệ tọa độ cố định trực giao bằng cách sử dụng bộ ba số thực (x, y, z). Cũng có thể được cho bằng một cặp số (x, y), nhưng được diễn giải là bộ ba với z=0.

b) Hướng có thể được xác định theo một trong hai cách. Một hướng tổng quát trong không gian ba chiều sẽ được đưa ra dưới dạng bộ bốn, được chuyển thành một bộ bốn số <c, su, sv, sw> trong đó (u, v, w) là trục quay, còn c và s lần lượt là cô sin và sin của nửa góc quay. Ngoài ra, một phép quay quanh trục z chỉ có thể được cho dưới dạng góc quay quanh trục đó, với góc được đo bằng radian.

c) Vị trí và hướng của rô bốt di động được xác định theo hệ tọa độ chuẩn của nó như được chỉ định trong TCVN 14446 (ISO 19649) và TCVN 13697 (ISO 9787).

d) Dữ liệu hình học vật thể 2D và 3D - được chọn từ các tiêu chuẩn hiện có.

Ngoài ra, khung chuẩn hệ mô đun có thể định nghĩa các hướng dẫn hoặc giới hạn, cách dữ liệu đầu vào/ đầu ra đến/ từ các mô đun nên được cấu trúc như thế nào.

Nhà sản xuất mô đun nên chọn các kiểu dữ liệu và cấu trúc dữ liệu phù hợp từ phạm vi được phép trong định nghĩa khung chuẩn hệ mô đun cho mô đun của mình. Thông tin về các kiểu dữ liệu và cấu trúc dữ liệu sẽ được nêu trong mô tả mô đun (xem Phụ lục B để biết ví dụ về các mô đun).

5 Quy định về an toàn và bảo mật

5.1 Yêu cầu chung

Điều này cung cấp hướng dẫn về cách các yêu cầu từ các tiêu chuẩn an toàn và bảo mật đã công bố có thể được áp dụng khi thiết kế các mô đun và các hệ thống dạng mô đun. Nội dung của điều này không được sử dụng như một sự biện minh cho việc không tuân thủ các tiêu chuẩn an toàn và bảo mật hiện hành.

CHÚ THÍCH 1: Có thể đánh giá độ an toàn ở cấp độ của một mô đun đơn lẻ (thường do nhà sản xuất mô đun thực hiện) và ở cấp độ của hệ thống rô bốt dịch vụ (thường do đơn vị tích hợp giải quyết).

An toàn và bảo mật là các khía cạnh thiết kế khác nhau, có thể ảnh hưởng lẫn nhau trong thiết kế rô bốt và trong thiết kế mô đun kiểu rô bốt. Vi phạm bảo mật trong hệ thống rô bốt và/ hoặc mô đun rô bốt có thể dẫn đến các mối nguy liên quan đến an toàn. Do đó, thông qua đánh giá rủi ro, nhà sản xuất mô đun rô bốt nên xem xét khả năng xuất hiện các mối nguy do các thuộc tính liên quan đến bảo mật gây ra trong các trường hợp sử dụng dự kiến, là đối tượng phải giảm thiểu thông qua thiết kế mô đun.

Lỗ hổng bảo mật trong một mô đun của hệ thống rô bốt dịch vụ có thể kéo theo vi phạm bảo mật cho toàn bộ hệ thống rô bốt dịch vụ, điều đó có thể dẫn đến các mối nguy. Nhà sản xuất mô đun phải nhận thức được các lỗ hổng bảo mật của mô đun có thể lan truyền qua hệ thống rô bốt. Vì lý do này, các khía cạnh an toàn và bảo mật cần được giải quyết để đảm bảo rằng các nhà thiết kế rô bốt tính đến chúng trong thiết kế mô đun của họ.

Các tiêu chuẩn an toàn hiện hành áp dụng cho rô bốt và hệ thống rô bốt gồm:

- TCVN 7383 (ISO 12100) về đánh giá rủi ro và giảm rủi ro của máy,
- TCVN 13229-1 (ISO 10218-1) và 13229-2 (ISO 10218-2), và TCVN 13700 (ISO/TS 15066) về rô bốt công nghiệp,
- TCVN 13231(ISO 13482) về rô bốt chăm sóc cá nhân,
- IEC/TR 60601-4-1, IEC 80601-2-77 và IEC 80601-2-78 về các đặc điểm khác nhau của rô bốt y tế,
- ISO 13849-1, sê-ri IEC 61508 và IEC 62061 về an toàn chức năng.

Phần mềm hệ thống rô bốt hệ mô đun có thể tham gia vào nhiều mô đun khác nhau của rô bốt. ISO/IEC/IEEE 12207:2017 và ISO/IEC/IEEE 15288:2015 đã xác định các quy trình vòng đời (chu trình thực hiện) để phát triển phần mềm nhằm đảm bảo đạt được chất lượng yêu cầu. IEC 61508-3 chỉ định các yêu cầu về an toàn cho phần mềm là một phần trong phần liên quan đến an toàn của hệ thống điều khiển. Các yêu cầu về an toàn cho phần mềm chỉ áp dụng cho các phần liên quan đến an toàn của phần mềm và được trình bày trong 7.2 và 7.4.

Khi áp dụng cách thiết kế hệ mô đun, khả năng tăng cường để cấu hình lại hệ thống rô bốt dịch vụ cho nhiều ứng dụng phải được tính đến trong quy trình đánh giá rủi ro và giảm rủi ro được mô tả trong TCVN 7383 (ISO 12100) để đảm bảo rằng các yêu cầu về an toàn được đáp ứng ngay cả sau khi thêm/xóa/cấu

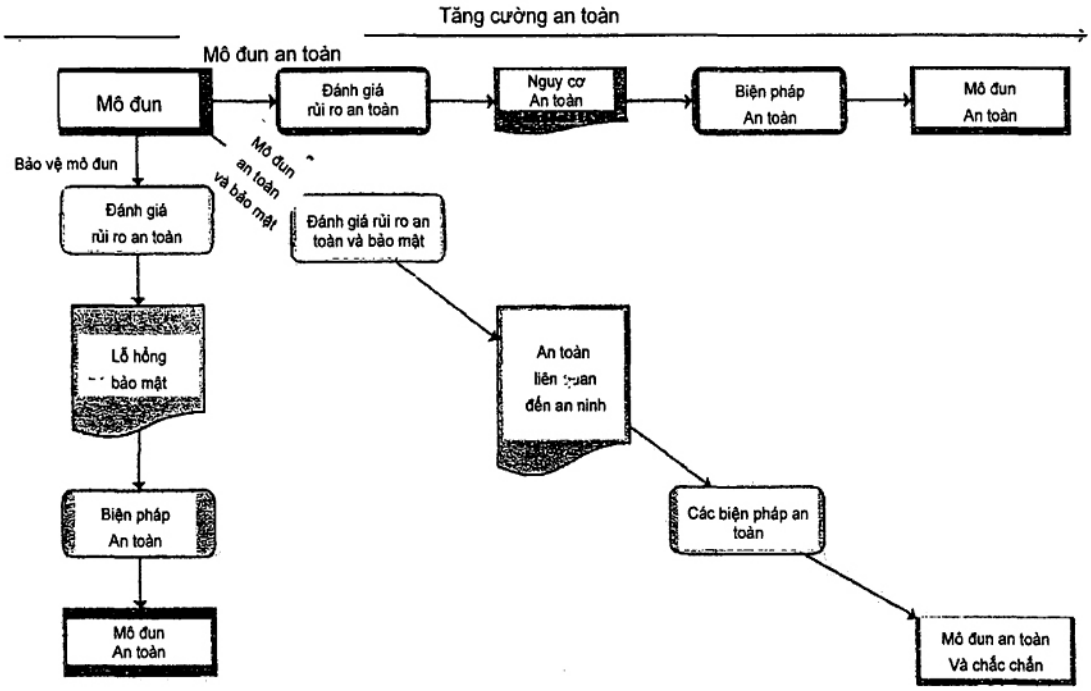
hình lại các mô đun, ví dụ bằng cách xem xét lại đánh giá rủi ro sau khi cấu hình lại. Các yêu cầu này có thể áp dụng ở cấp độ hệ thống cũng như ở cấp độ mô đun. Ngoài đánh giá rủi ro dựa trên an toàn thông thường, nhà thiết kế và/hoặc tích hợp rô bốt dịch vụ sẽ kết hợp đánh giá rủi ro bảo mật để đánh giá hậu quả đối với an toàn. Ví dụ, tình huống nguy hiểm có thể được giảm thiểu bằng cách thêm một mô đun. Tuy nhiên, sau bất kỳ thay đổi nào trong cấu trúc hệ mô đun của hệ thống rô bốt, các rủi ro sau khi thực hiện cấu hình lại hệ mô đun phải được đánh giá lại về an toàn và bảo mật.

Nên áp dụng các tiêu chuẩn sau đây khi đánh giá bảo mật của mô đun và hệ thống rô bốt:

- ISO/TR 22100-4 liên quan đến các đặc điểm bảo mật công nghệ thông tin cho máy
- ISO/IEC 27032 cho các hướng dẫn chung về an ninh mạng
- IEC/TS 62443-1-1 về thuật ngữ, khái niệm và mô hình
- IEC 62443-2-1 liên quan đến các chương trình bảo mật cho tự động hóa công nghiệp
- IEC 62443-3-3 về các cấp độ bảo mật của các hệ thống điều khiển
- NIST SP 800-154 về mô hình hóa mối đe họa lên hệ thống lấy dữ liệu làm trung tâm
- NIST SP 800-160 tập 1 và 2 về kỹ thuật bảo mật hệ thống

Hình 2 chỉ ra các rủi ro về an toàn và bảo mật có liên quan như thế nào và cách giải quyết chúng. Các nhà sản xuất và tích hợp mô đun (và các nhà thiết kế khung chuẩn cho mô đun, nếu có) phải tuân theo các quy tắc và yêu cầu được thiết lập trong các tiêu chuẩn an toàn có thể áp dụng hiện hành. Điều này được thể hiện bằng đường nằm ngang trên Hình 2. Các rủi ro về bảo mật đối với một mô đun phải được đánh giá theo cùng một mục đích sử dụng, sử dụng sai mục đích có thể lường trước và "giới hạn của máy" (theo ISO 12100:2010, 5.3) như đã được sử dụng khi phân tích an toàn cho mô đun. Quá trình đánh giá và giảm thiểu rủi ro về bảo mật (đường thẳng đứng trên Hình 2) phải được thực hiện theo quy trình lặp lại: song song với các bước 1 và 2 của Hình 1 trong ISO 12100:2010, Điều 4 hoặc vào cuối quy trình tương ứng. Quy trình tích hợp để đánh giá và giảm thiểu cả rủi ro bảo mật và rủi ro an toàn (đường chéo trên Hình 2) phải được thực hiện theo một quy trình lặp lại. Trong trường hợp việc triển khai các biện pháp bảo mật xung đột với việc triển khai chức năng an toàn dự định (để đáp ứng yêu cầu an toàn), việc giảm thiểu rủi ro an toàn sẽ được ưu tiên, trong khi vẫn giảm thiểu rủi ro bảo mật ở mức hợp lý nhất có thể.

CHÚ THÍCH 2: Nhà sản xuất mô đun có thể thử một triển khai khác của chức năng an toàn tương ứng nếu vẫn đáp ứng yêu cầu về an toàn hoặc có thể ước tính biện pháp bảo mật để sử dụng một cách hợp lý mà không gây cản trở chức năng an toàn.



Hình 2 – Các lưu ý về rủi ro an toàn và bảo mật cho các mô đun rô bốt

Nhà sản xuất mô đun nên xem xét các trường hợp sử dụng dự kiến của mô đun và công nghệ mà mô đun sử dụng để xác định các yêu cầu cần thiết cho nhiều miền ứng dụng khác nhau (ví dụ: cơ học, điện từ, phần mềm, bảo mật, môi trường, sinh học, hóa học, khả năng sử dụng, v.v.). Ngoài ra, nhà sản xuất mô đun phải xác định và liệt kê các trường hợp sử dụng được xem xét với các hạn chế và loại trừ cụ thể. Mặc dù hệ mô đun có thể không được thể hiện rõ ràng trong phạm vi sử dụng của các tiêu chuẩn hiện hành trong các miền ứng dụng dự kiến, nhưng các nguyên tắc được trình bày trong các tiêu chuẩn hiện hành có thể hữu ích để đưa ra các yêu cầu và phương pháp thử nghiệm mô đun phù hợp. Xem Phụ lục D để biết thông tin chi tiết về thử nghiệm các mô đun kiểu rô bốt.

Nhà tích hợp mô đun nên xem xét các thông tin sau:

- Mối quan hệ với hệ thống bên ngoài (bố cục vật lý, giao diện, v.v...);
- Hướng dẫn bảo trì cho các cấp độ mô đun và hệ thống.

5.2 An toàn cấp độ hệ thống rô bốt

Các phương pháp được sử dụng để đánh giá độ an toàn của một hệ thống rô bốt chứa các mô đun rô bốt không khác biệt với các phương pháp được sử dụng để đánh giá các hệ thống rô bốt không có mô đun, và chúng được công bố trong các tiêu chuẩn hiện hành.

Các nhà phát triển khung chuẩn cho rô bốt dịch vụ hệ mô đun chịu trách nhiệm:

- Thiết kế kiến trúc và tổ hợp của các mô đun kiểu rô bốt dịch vụ khác nhau;
- Đảm bảo kết nối và xử lý đúng các tín hiệu an toàn giữa các mô đun;

- Đánh giá độ an toàn cần thiết của rô bốt cho các ứng dụng có trường hợp sử dụng điển hình.

CHÚ THÍCH 1: Các ứng dụng có trường hợp sử dụng điển hình có thể bao gồm các cấp độ khác nhau về an toàn, bảo mật, an toàn kết hợp và bảo mật, và chất lượng.

CHÚ THÍCH 2: Tín hiệu đề cập đến cả tín hiệu có dây cứng như tín hiệu dừng khẩn cấp vào hoặc ra khỏi mô đun và cả dữ liệu được trao đổi qua mạng có dây hoặc không dây, trong trường hợp đó mạng phải đáp ứng các yêu cầu về an toàn chức năng.

Các nhà sản xuất mô đun phải chịu trách nhiệm chỉ định các ứng dụng có trường hợp sử dụng dự kiến cho các mô đun.

Các nhà tích hợp mô đun phải chịu trách nhiệm về:

- Tuân thủ các tiêu chuẩn an toàn rô bốt hiện hành được đề cập trong 5.1.
- Tính toán các trường hợp sử dụng theo kế hoạch của hệ thống, được so sánh về mức độ liên quan và tính đóng với các trường hợp sử dụng dự kiến do nhà sản xuất mô đun đưa ra.
- Tuân thủ các hướng dẫn an toàn do nhà sản xuất mô đun quy định, bao gồm cả các yêu cầu về điều kiện sử dụng.

Nếu hệ thống rô bốt hoặc các ứng dụng có trường hợp sử dụng thay đổi, thì quá trình đánh giá rủi ro sẽ được thực hiện để tính đến các thay đổi này. Các ví dụ được trình bày trong Phụ lục C. Nếu việc thay đổi các bộ phận của hệ thống rô bốt hệ mô đun được dự định sẽ do người dùng cuối thực hiện thì đánh giá rủi ro phải bao gồm các mối nguy hiểm từ các cấu hình có thể thiết lập.

CHÚ THÍCH 3: Các giới hạn sử dụng thích hợp và các biện pháp phòng ngừa an toàn bắt buộc hoặc các bước phải theo là một phần của hướng dẫn sử dụng của hệ thống rô bốt.

Các nhà phát triển khung chuẩn cho rô bốt dịch vụ hệ mô đun phải thực hiện các biện pháp thiết kế nhằm hỗ trợ việc giảm rủi ro để đảm bảo các điều sau:

- Các tín hiệu an toàn phổ quát và trạng thái lỗi cùng các quy tắc về cách sử dụng và lan truyền chúng;
- Các tính năng an toàn hoặc mức an toàn tối thiểu mà tất cả các mô đun nên duy trì;
- Các mục cốt lõi sẽ được đưa vào tài liệu về đặc tính an toàn.

5.3 An toàn cấp độ mô đun

Thiết kế của mô đun phải tính đến các tiêu chuẩn hiện hành về an toàn điện và cơ (xem Phụ lục D đối với các mô đun rô bốt thử nghiệm). Yêu cầu an toàn đối với phần mềm được thảo luận trong 5.4.

Nếu động cơ được thiết kế để có chức năng dừng, mô đun phải cung cấp chức năng an toàn tương ứng phù hợp với IEC 61800-5-2.

Để tránh lỗi do truyền thông giữa các mô đun, hệ thống nên sử dụng truyền thông kênh đen (xem IEC 62280 và IEC 61784-3). Trong trường hợp này, khối độ tin cậy của mô đun phải được thiết kế an toàn và một đường truyền nên được xây dựng đảm bảo độ tin cậy của chức năng an toàn.

Mức hiệu quả (PL) hoặc mức độ toàn vẹn an toàn (SIL) sẽ được chỉ định cho các chức năng an toàn thực hiện. Các PL / SIL này có thể được sử dụng để đánh giá hiệu quả tổng thể của một chức năng an toàn đối với hệ thống rô bốt hoàn chỉnh. Nhà sản xuất mô đun nên công bố PL hoặc SIL cho tất cả các chức năng an toàn được chia sẻ bởi một mô đun với các mô đun khác. Các tín hiệu trong một mô đun không liên quan đến an toàn trong mô đun đó nhưng vẫn có thể hữu ích và được truyền tới các mô đun khác cho các chức năng liên quan đến an toàn.

Quá trình thiết kế các mô đun rô bốt có thể khác với thiết kế hệ thống thông thường vì nhà thiết kế/nhà sản xuất mô đun không có ứng dụng cụ thể cuối cùng tại thời điểm thiết kế (chỉ biết các tình huống có trường hợp sử dụng điển hình).

Nhà sản xuất mô đun rô bốt có thể sử dụng các bước sau để đảm bảo các yêu cầu thiết kế an toàn phù hợp và đầy đủ được bao gồm:

1. Xác định các trường hợp sử dụng dự kiến và cho mỗi trường hợp sử dụng, hãy mô tả càng nhiều chi tiết liên quan càng tốt.
2. Một thiết kế hệ thống rô bốt giả định nên được thực hiện cho từng trường hợp sử dụng. Tất cả các ứng dụng có thể dự kiến của một mô đun phải được xem xét. Việc sử dụng sai có thể lường trước của một mô đun cũng phải được xem xét.

   CHÚ THÍCH 1: Giả định rằng hệ thống có giám sát an toàn có thể được thực hiện nếu cần thiết (xem7.2 và 7.4).
3. Đối với mỗi ứng dụng có trường hợp sử dụng dự kiến, cần xác định các mối nguy tiềm ẩn (ISO 12100:2010, Phụ lục B, bao gồm danh sách các mối nguy hiểm tiềm ẩn cần được xem xét).
4. Để thực hiện đánh giá rủi ro mất an toàn, cần xem xét mô đun như một mô đun riêng lẻ và những mối nguy hiểm tiềm ẩn mà nó có thể gây ra trong các ứng dụng có trường hợp sử dụng dự kiến.

   Các yêu cầu về an toàn của mô đun phải dựa trên một số ứng dụng dự kiến với trường hợp sử dụng xấu nhất được giả định.
5. Nhà sản xuất mô đun phải hoàn thành đánh giá rủi ro an toàn cho mỗi trường hợp sử dụng dự kiến, để xác định PL phù hợp cho bất kỳ chức năng liên quan đến an toàn nào có liên quan trong mô đun. Có thể xây dựng các chức năng liên quan đến an toàn cục bộ trong mô đun để xử lý chức năng này - xem "giám sát an toàn" trong 7.2.

CHÚ THÍCH 2: Không phải tất cả các bước đều cần thiết trong mọi tình huống.

Nhà sản xuất mô đun phải cung cấp các trường hợp sử dụng dự kiến cùng các giả định của chúng và cung cấp thông tin sau cho các nhà tích hợp mô đun:

- Thông tin để sử dụng mô đun.
- Các điều kiện môi trường mà mô đun có thể được vận hành an toàn.
- Thông tin về các chức năng liên quan đến an toàn trong mô đun.

- Thông tin về dữ liệu mà mô đun cung cấp cho các mô đun khác, có thể có ý nghĩa đối với an toàn bên ngoài mô đun (ví dụ: trong giám sát an toàn).

CHÚ THÍCH 3: Các yêu cầu về an toàn cho các chức năng như giao diện người vận hành và dừng khẩn cấp được cung cấp trong IEC 60204-1 và có thể liên quan đến các mô đun.

Ví dụ, hai triển khai có thể có của hệ thống an toàn của nền tảng rô bốt di động được giới thiệu dưới đây để chứng minh rằng các mô đun có nhiều tính năng hơn (liên quan đến an toàn) sẽ dễ tích hợp hơn và có thể sử dụng cho các tình huống thực tế.

VÍ DỤ: Hai mô đun tổng hợp, do hai nhà sản xuất khác nhau cung cấp, có các tính năng sau:

- Nền tảng 1 có các động cơ được giới hạn tốc độ tối đa của nền tảng ở mức 1 m/s. Bộ điều khiển nền tảng chấp nhận tốc độ di chuyển mong muốn làm đầu vào và đưa ra tốc độ hiện tại, nhưng cả hai tín hiệu đều không thuộc loại liên quan đến an toàn và không có xếp hạng mức hiệu năng.
- Nền tảng 2 có thể đạt tốc độ tối đa là 2 m/s. Bộ điều khiển nền tảng cung cấp khả năng kiểm soát tốc độ liên quan đến an toàn với mức hiệu năng cao. Do đó, đầu vào tốc độ mong muốn và đầu ra tốc độ hiện tại đều thuộc loại liên quan đến an toàn.

Một nhà tích hợp rô bốt thiết kế một rô bốt di động với Nền tảng 1 có hệ thống an toàn đơn giản bao gồm các mô đun máy quét laser có trường bảo vệ cố định, có thể dừng xe kịp thời khi xe chạy ở tốc độ 1 m/s.

Khi sử dụng Nền tảng 2 thay vì Nền tảng 1, nhà tích hợp rô bốt nên tăng đáng kể các trường bảo vệ của máy quét laser để phù hợp với tốc độ tối đa có thể đạt được là 2 m/s. Thay vào đó, nhà tích hợp rô bốt quyết định sử dụng chức năng kiểm soát tốc độ liên quan đến an toàn của Nền tảng 2. Trong trường hợp này, các trường bảo vệ tối đa chỉ cần thiết khi nền tảng thực sự chạy ở tốc độ cao. Đối với các thao tác chậm khi về trạm hoặc ghép nối, các trường bảo vệ có thể được giảm bớt.

Ví dụ này chứng minh rằng hệ thống có khả năng thích ứng tốt hơn với các yêu cầu thay đổi về môi trường với các tính năng an toàn cần thiết khi sử dụng Nền tảng 2.

CHÚ THÍCH 4: Việc sử dụng điều khiển tốc độ và chuyển đổi các trường bảo vệ đòi hỏi cả mô đun máy quét laser và mô đun giám sát an toàn đều hỗ trợ chức năng này.

5.4 Đặc điểm chung của bảo mật

Bảo mật cấp độ mô đun phải đảm bảo rằng các mô đun riêng lẻ có khả năng chống lại truy cập trái phép để ngăn chặn các cuộc tấn công ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính khả dụng của mô đun như:

- truy cập trái phép vào dữ liệu nội bộ (có thể ảnh hưởng đến sở hữu trí tuệ hoặc dữ liệu cá nhân);
- truy cập trái phép và thay đổi cấu hình mô đun và cài đặt tham số nội bộ (cũng có thể ảnh hưởng đến an toàn);
- các cuộc tấn công gây hư hỏng cho mô đun hoặc hệ thống rô bốt hệ mô đun hoặc ngăn cản việc sử dụng bình thường.

Việc can thiệp vào các mô đun của hệ thống rô bốt sẽ trở thành mối nguy hiểm về an toàn vì hệ thống rô bốt hoặc các bộ phận của nó có thể thực hiện các chuyển động không kiểm soát do hệ thống an toàn bị hư hại. Để xác nhận mức độ bảo mật của mô đun, xem Phụ lục D.

An ninh mạng là một lĩnh vực đang phát triển và cần được tính đến khi thiết kế mô đun, do đó, cần xem xét các phát triển mới nhất để đưa vào. Phương pháp thiết kế được đề xuất có điểm tương đồng mạnh mẽ với các bước được cung cấp trong các mục liên quan đến an toàn trước đây.

CHÚ THÍCH 1: Hiện tại không có mức hiệu quả bảo mật nào có thể tham khảo được.

Các biện pháp bảo vệ mô đun và rô bốt dịch vụ hệ mô đun phải được lựa chọn theo kết quả của đánh giá rủi ro bảo mật, có tính đến những điều sau:

- Tiếp xúc với những đối tượng xâm nhập tiềm ẩn (người trong cuộc và người ngoài cuộc);
- Tác hại tiềm ẩn có thể gây ra do truy cập trái phép (ví dụ: ảnh hưởng đến tính khả dụng hoặc an toàn);
- Động cơ tiềm ẩn của những đối tượng xâm nhập để có được quyền truy cập (ví dụ: truy cập vào dữ liệu riêng tư có giá trị).

Để đạt được bảo mật cấp độ hệ thống, tất cả các mô đun được kết nối trao đổi dữ liệu phải là các mô đun có đủ khả năng bảo vệ để chống lại việc truy cập trái phép vào các cổng dữ liệu vật lý. Truyền thông nội bộ bên trong mô đun, truyền thông giữa các mô đun và truyền thông bên ngoài hệ thống rô bốt phải được xử lý khác nhau.

CHÚ THÍCH 2: Trong hầu hết các thiết bị an toàn hiện đại và các chức năng liên quan đến an toàn trong hệ thống máy móc và rô bốt, một số loại phần mềm truyền thông (và được nhúng) đều có mặt. Hầu như bất kỳ phần mềm nào cũng có khả năng bị ảnh hưởng theo cách mà hành vi và chức năng an toàn có thể bị thay đổi. Nếu một mô đun như vậy chia sẻ dữ liệu với các mô đun khác hoặc bên ngoài hệ thống rô bốt, khả năng truy cập trái phép và ảnh hưởng có thể lớn hơn. Điều 7 mô tả chi tiết hơn về vấn đề này.

Tiêu chuẩn này sử dụng các cấp độ an toàn và bảo mật kết hợp để phân loại mô đun như sau:

1. Không cần an toàn hoặc bảo mật: Cấp độ này có thể áp dụng cho các rô bốt nhỏ và nhẹ không thể gây hại cho người và không được kết nối với bất kỳ hệ thống bên ngoài nào.
2. Cần bảo mật: Áp dụng khi mục đích sử dụng dự kiến của mô đun bao gồm các truyền thông bên trong rô bốt hoặc với các hệ thống bên ngoài. Điều 6 mô tả các biện pháp bảo mật liên quan đến phần cứng và Điều 7 mô tả các biện pháp liên quan đến phần mềm và truyền thông để đạt được tính bảo mật cho một môđun.
3. Trong một số trường hợp, có thể thiết kế một hệ thống an toàn nhưng tiềm ẩn nguy cơ không bảo mật; điều này sẽ phụ thuộc vào ứng dụng nếu được chấp nhận.
4. Cần có sự kết hợp giữa an toàn và bảo mật: Một hệ thống chỉ có thể được coi là an toàn và bảo mật nếu cả yêu cầu về an toàn và yêu cầu về bảo mật đều được giải quyết. Hình 2 cho thấy quy trình cần tuân theo để đảm bảo đánh giá rủi ro an toàn và bảo mật đầy đủ.

CHÚ THÍCH 3: Một hệ thống chỉ có phần cứng mà không có phần mềm, giống như công tắc an toàn, đây là một trong số ít trường hợp ngoại lệ có thể được coi là an toàn mà không thực sự bảo mật.

5.5 Các bước thiết kế an toàn trong mô đun

Nhà sản xuất mô đun rô bốt nên sử dụng các bước sau để đảm bảo các yêu cầu thiết kế bảo mật phù hợp và đầy đủ:

1. Xác định các trường hợp sử dụng cho mô đun theo quan điểm bảo mật. Các trường hợp sử dụng này có thể tương tự như các trường hợp được xác định cho mục đích an toàn, nhưng cũng có thể khác nhau.
2. Cần xem xét các mục đích sử dụng dự kiến và các ứng dụng tiềm năng của mô đun.

   CHÚ THÍCH: Giả định rằng hệ thống có giám sát bảo mật (xem 7.2 và 7.4) có thể được đưa ra nếu cần.
3. Nhà thiết kế nên hoàn thành đánh giá rủi ro bảo mật cho từng trường hợp sử dụng để đưa ra các yêu cầu bảo mật mà mô đun nên duy trì để tạo điều kiện thuận lợi cho bảo mật mô đun và hệ thống.
4. Phần mềm trong mô đun phải tuân thủ các yêu cầu bảo mật tại 7.4.
5. Kiểm tra xem các hướng dẫn về trao đổi dữ liệu an toàn có được cung cấp như trình bày trong 7.4 không.
6. Kiểm tra các hướng dẫn về phần cứng trong 5.7 để bảo vệ mô đun khỏi truy cập trái phép.
7. Đánh giá rủi ro bảo mật nên được tiến hành độc lập trên từng mô đun và các hậu quả được đánh giá trong các tình huống sử dụng được mô tả trong bước 2.

5.6 Bảo mật vật lý của mô đun

Nhà sản xuất mô đun cần cân nhắc các khía cạnh sau đây về bảo mật vật lý cho thiết kế mô đun khi tích hợp chúng cho hệ thống rô bốt hệ mô đun:

- Bảo mật cổng truyền thông
- Truy cập vật lý vào các thành phần bên trong từ bên ngoài

CHÚ THÍCH: Các mô đun có thể truyền qua hệ thống bus đến các mô đun lân cận. Do đó, vi phạm bảo mật có thể lan truyền từ mô đun này sang mô đun khác.

Các nhà sản xuất và tích hợp mô đun phải xem xét các biện pháp sau để hạn chế quyền truy cập vào cổng truyền thông của mô đun hoặc hệ thống, ví dụ:

- Cảm biến chốt (không cần bảo mật nhưng cần biết trạng thái mở hay đóng)
- Khóa cơ khí với chìa khóa vật lý
- Khóa cơ khí với bộ dẫn động chốt

Các mô đun không có biện pháp bảo mật chỉ được chấp nhận trong môi trường được bảo vệ như môi trường phòng thí nghiệm nghiên cứu nội bộ hoặc đối với các rô bốt dịch vụ nhỏ và nhẹ.

5.7 An ninh mạng của mô đun

Một mô đun (hoặc phần cứng và phần mềm) phải:

- Cấm can thiệp trái phép;
- Cung cấp bảo mật cho dữ liệu được lưu trữ, xử lý và trao đổi giữa các mô đun;
- Cung cấp bảo mật truyền thông.

CHÚ THÍCH 1: Sự cần thiết của việc áp dụng biện pháp an ninh mạng phụ thuộc vào mục đích sử dụng của mô đun.

An ninh mạng của một mô đun phải được thiết kế để đạt được các mục tiêu bảo mật sau: tính bí mật, tính toàn vẹn và tính khả dụng. Khi thực hiện đánh giá rủi ro an ninh mạng và giảm rủi ro, cần cân nhắc những điều sau:

- Ví dụ về các biện pháp bảo mật: Khởi động an toàn, xác thực (ví dụ: mật khẩu), mã hóa dữ liệu;
- Ví dụ về các biện pháp bảo toàn: Kiểm soát và cấp phép truy cập, kiểm tra tổng;
- Ví dụ về các biện pháp bảo toàn và bảo mật: Bảo mật dữ liệu, Truyền thông an toàn;
- Ví dụ về các biện pháp bảo đảm tính khả dụng: Cập nhật mã an toàn, băng thông truyền thông đầy đủ, dự phòng.

CHÚ THÍCH 2: Các đặc điểm bảo mật chung cho các hệ thống tự động hóa công nghiệp được trình bày trong loạt tiêu chuẩn IEC 62443. Một tiêu chuẩn đang được phát triển về các đặc điểm bảo mật của máy móc; IEC/TR 63074 trình bày các đặc điểm bảo mật liên quan đến an toàn chức năng của các hệ thống điều khiển.

6 Đặc điểm phần cứng trong thiết kế mô đun

6.1 Yêu cầu chung

Điều này mô tả các yêu cầu và hướng dẫn để cho phép khả năng tương tác và khả năng tái sử dụng của các mô đun với các đặc điểm phần cứng gồm cả các mô đun phần cứng. Đối với các mô đun có các đặc điểm phần cứng, Bảng 3 cho thấy các vấn đề kết nối chính cần được xem xét để hiện thực hóa một khung chuẩn cho thiết kế hệ mô đun hiệu quả và do đó đạt được các yêu cầu về khả năng tương tác, an toàn và bảo mật như được trình bày trong tiêu chuẩn này. Các ví dụ về các mô đun có các đặc điểm phần cứng được hiển thị cùng với cách giải quyết các vấn đề kết nối. Thiết kế một mô đun phần cứng hoặc một mô đun có các đặc điểm phần cứng, chẳng hạn như cơ cấu truyền động, có thể yêu cầu cân nhắc đến tính an toàn, bảo mật, nguồn điện, tín hiệu cũng như cấu trúc cơ học.

CHÚ THÍCH: Các vấn đề kết nối của các mô đun phần cứng hoặc các mô đun có đặc điểm phần cứng có thể mang tính vật lý (ví dụ: Nguồn điện, Dữ liệu) hoặc có thể đề cập đến các tương tác trừu tượng hơn (ví dụ: An toàn, Bảo mật, Môi trường, Cơ học). Nếu một mô đun được kết nối với Bảo mật, mô đun này có các vấn đề bảo mật hoặc trao đổi dữ liệu theo một cách nào đó với các mô đun liên quan đến bảo mật khác.

Bảng 3 – Các vấn đề kết nối đối với khung chuẩn hệ mô đun qua các mô đun ví dụ

Mô đun/ tương tác	Môi trường	Cơ học	Dữ liệu	Nguồn	An ninh	An toàn
Truyền động	√	√	√	√	√	√
Nguồn điện			(√)	√	√	√
Cảm biến	√	√	√	√	√	√
Máy tính			√	√	√	√
Người giám sát	√		√	√	√	√
Giao diện người dùng	√		√	√	√	√

6.2 Yêu cầu và hướng dẫn cho các mô đun có đặc điểm phần cứng

6.2.1 Mặt lắp ghép cơ khí

6.2.1.1 Yêu cầu chung

Mô đun phải được cung cấp cùng với thông số kỹ thuật của mặt lắp ghép cơ khí của nó và các đầu nối, ví dụ:

- Thông số kỹ thuật các đầu nối và mặt lắp ghép;
- Thông số kỹ thuật các đầu nối có phần giữ chỗ (các đầu nối mù hoặc rỗng để kết nối không cần thiết cho mô đun);
- Thông số kỹ thuật các kích thước vật lý của đầu nối cho các yêu cầu khác nhau về độ bền vật lý và kích thước, ví dụ cho mục đích sử dụng dự kiến cho các bộ phận khác nhau của tay máy;
- Thông số kỹ thuật liên kết cơ học cho vòng lặp của bus dữ liệu và/hoặc nguồn điện;
- Thông số kỹ thuật các mặt lắp ghép cho phép bus dữ liệu hoặc nguồn điện được lặp qua mô đun, ngay cả khi bản thân mô đun không yêu cầu kết nối với chúng (ví dụ trong trường hợp liên kết cơ học).

CHÚ THÍCH 1: Mặc dù nên tích hợp các đầu nối trong mô đun, nhưng nó đưa ra thách thức thiết kế cụ thể đối với việc kết hợp chuyển động vật lý của việc ghép nối và tách rời mô đun về mặt cơ khí, đồng thời kết nối và ngắt kết nối các đầu nối cho dữ liệu, nguồn, an toàn và bảo mật để duy trì hoạt động dự kiến của chúng. Nếu các đặc điểm thiết thực của thiết kế này không đáp ứng các yêu cầu cho mục đích sử dụng, mô đun có thể chịu (các) rủi ro về an toàn và hiệu quả, cuối cùng dẫn đến trục trặc và lỗi.

Thử nghiệm và xác nhận thích hợp việc ghép nối và tách rời mô đun với các mô đun khác nên được thực hiện. Nếu có, thông tin để sử dụng phải nêu rõ rằng cần phải thử nghiệm và xác nhận. Các mô đun phải kèm theo thông tin để cho phép kiểm tra và xác nhận việc ghép nối và tách rời các mô đun với nhau. Thông tin để sử dụng phải bao gồm các thông tin để đảm bảo khả năng kết nối và chức năng giữa các mô đun có đặc điểm phần cứng, ví dụ:

- Căn chỉnh mô đun, định vị mô đun và khóa mô đun với độ cứng vững mong muốn trong trạng thái tĩnh và các trường hợp chuyển động động theo kế hoạch;
- Khẳng định dữ liệu, tín hiệu và kết nối nguồn không bị hỏng trong quá trình định vị cơ học và quá trình khóa giao diện của mô đun;
- Các cơ cấu kết nối/ khóa cơ khí để đạt được độ chính xác và độ cứng vững được chỉ định trong đầu ghép nối cơ khí cho các trường hợp sử dụng dự kiến của mô đun.

Xem xét mục đích sử dụng của mô đun và các trường hợp sử dụng được chỉ định, số lần mô đun có thể được ngắt kết nối và kết nối lại trong thời gian sử dụng được chỉ định của mô đun. Ví dụ, các thiết kế sau có thể được sử dụng khi có thể:

- Sử dụng kiểu lắp có độ dôi tăng dần để đưa các điểm tiếp xúc vật lý lại với nhau mà không bị hư hại;
- Sử dụng các cấu trúc đồng trục và/ hoặc hình nón để giảm chuyển động chéo hoặc chuyển động ngang trong quá trình ghép nối để tránh mài mòn và hư hỏng các điểm tiếp xúc;
- Sử dụng cấu trúc hình xuyến để tạo ra tiếp xúc đa điểm làm tăng miền phân bố của kết nối vật lý nhằm nâng cao độ chính xác trong ghép nối cơ khí;
- Sử dụng vật liệu và cấu trúc phù hợp tạo ra các kết nối cơ khí thích ứng tốt hơn cho việc phân phối lực cơ học qua một cấu trúc mở rộng để tránh hư hỏng cục bộ khi đặt lực tại một điểm duy nhất.

CHÚ THÍCH 2: Các tiêu chuẩn về mặt lắp ghép cho rô bốt công nghiệp có thể được sử dụng cho các mô đun của rô bốt dịch vụ, ví dụ: TCVN 13234-1, -2 (ISO 9409-1, -2) và TCVN 13230 (ISO 11593).

Các nhà sản xuất mô đun phải cung cấp thông số kỹ thuật của mặt lắp ghép cơ khí để các nhà sản xuất hoặc nhà tích hợp mô đun khác sử dụng. Điều này có thể bao gồm:

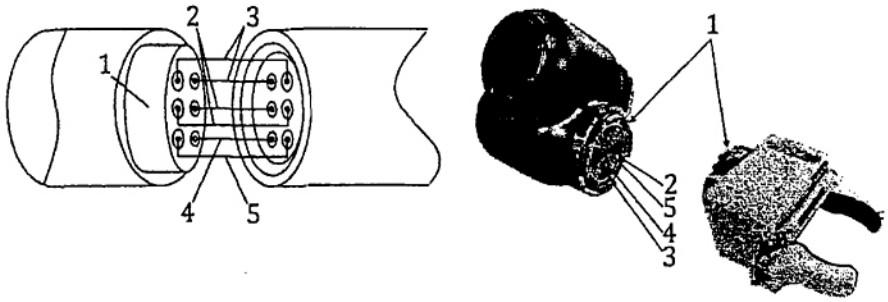
- Dữ liệu thiết kế CAD của các bộ phận cơ khí;
- Nhà sản xuất và số hiệu của phích cắm;
- Cách bố trí các chân cắm.

6.2.1.2 Độ chính xác và độ tin cậy của kết nối

Trong thiết kế rô bốt dịch vụ hệ mô đun, các kết nối giữa các mô đun phải có các đặc tính kết nối cho mục đích sử dụng dự kiến sau đây, ví dụ về các đặc điểm này được thể hiện trên Hình 3:

- Nguồn điện
- Dữ liệu
- Bảo mật
- An toàn
- Cơ cấu

Các mô đun liên quan đến an toàn phải đảm bảo an toàn để kết nối chúng với nhau. Các mô đun phải quy định độ chính xác khi kết nối chúng với nhau.



a) Kết nối giữa các khớp b) Kết nối giữa khớp và khâu tác động cuối

CHÚ DẪN:

1 cơ học
2 dữ liệu
3 nguồn
4 an ninh
5 an toàn

Hình 3 – Ví dụ về các đặc tính kết nối cần thiết trong một đầu nối hệ mô đun

Thông tin cho sử dụng phải bao gồm thông số kỹ thuật của các đầu nối hệ mô đun để đảm bảo độ tin cậy:

- Lượng dịch chuyển và xoay để hoạt động sau khi khớp được khóa. Nghĩa là, không thể bị long ra sau khi khớp đã được khóa;
- Các thông số về độ cứng vững và độ tin cậy của mặt lắp ghép mô đun. Độ mòn của các bề mặt cơ học để căn chỉnh và các kết nối tích hợp cho cấp nguồn, dữ liệu và an toàn để chịu được số chu kỳ ghép nối/ tách rời tối thiểu;
- Các đặc tính về độ bền của mặt lắp ghép mô đun. Trong các trường hợp sử dụng mà các mô đun thường xuyên được thay đổi hoặc có khả năng xảy ra các điều kiện khắc nghiệt như bụi bẩn và quá tải, mô đun phải được kiểm tra và xác nhận cho số chu kỳ đã chỉ định. Nhà sản xuất phải chỉ định số chu kỳ tối thiểu.

Các nhà sản xuất mô đun ít nhất phải đáp ứng các yêu cầu được xác định trong khung chuẩn hệ mô đun hoặc xác định thông số kỹ thuật của riêng họ để đáp ứng các ứng dụng có trường hợp sử dụng dự kiến của họ.

6.2.1.3 Độ cứng vững của kết nối

Mô đun và mặt lắp ghép mô đun phải có đủ độ cứng vững để truyền lực và mô men xoắn tĩnh và động từ mô đun này sang mô đun khác thông qua quy trình kiểm tra và xác nhận, thường được gọi là thiết kế

trọn gói. Để hạn chế lượng biến dạng hình học của mô đun so với đầu kia của mô đun, mô men xoắn và lực tải tối đa có thể được chỉ định trên ba trục (x, y, z) tại mặt lắp ghép hoặc ở đầu kia của mô đun.

Lực và/ hoặc mô men xoắn có thể áp dụng phải được chỉ định cho mô đun, bao gồm cả mặt lắp ghép của nó, để đáp ứng các yêu cầu sau:

- Biến dạng hình học tối đa ở đầu kia của mô đun thực phải nhỏ hơn một lượng đã được chỉ định.
- Biến dạng xoắn tối đa khi chịu tải trọng xoắn lớn nhất phải nhỏ hơn một lượng đã được chỉ định.

6.2.1.4 Các đầu nối và kết nối cơ khí

Mô đun phải có thể được ghép nối bằng ít dụng cụ nhất hoặc không cần dụng cụ nếu có thể. Nếu mô đun tương đối nhỏ, có thể ghép nối thủ công (tức là không cần dụng cụ hỗ trợ). Đối với các mô đun nặng hơn, khi cần sử dụng thiết bị nâng, mặt lắp ghép cơ khí phải được thiết kế để chấp nhận các lực lớn hơn khi lắp, va chạm giữa các mặt lắp ghép hoặc tiếp xúc tốc độ cao, v.v... mà không gây hư hỏng cho mặt lắp ghép cơ khí.

Nhà sản xuất nên khuyến nghị thử nghiệm theo chỉ định để đánh giá độ bền của phương pháp ghép nối/tách rời áp dụng trong các ứng dụng có trường hợp sử dụng cụ thể (xem Phụ lục D).

Nếu các đầu nối được tích hợp trong mô đun, cần cung cấp hướng dẫn phù hợp để ghép nối/ tách rời mô đun một cách an toàn.

CHÚ THÍCH: Nên sử dụng loại đầu nối đặc biệt cho các giải pháp cáp đơn, đặc biệt là trong các ứng dụng điều khiển chuyển động và điều khiển động cơ trong đó đầu nối tích hợp mặt lắp ghép cơ khí, nguồn điện, dữ liệu và tín hiệu an toàn, và có hướng dẫn phù hợp để ghép nối/tách rời một cách an toàn.

Các đầu nối điện phải tuân thủ các yêu cầu được trình bày trong IEC 61076-1 và/hoặc IEC 61984 nếu thích hợp.

Việc lựa chọn và định vị các đầu nối riêng lẻ phải đảm bảo duy trì các yêu cầu sau:

- các quỹ đạo lực/ chuyển động phát sinh phải nằm trong giới hạn quy định;
- các yêu cầu về cung cấp năng lượng dạng điện, khí nén, thủy lực và cơ học;
- các yêu cầu về truyền dữ liệu và tính toàn vẹn của chúng;
- tuân thủ các yêu cầu an toàn có liên quan đã công bố (xem Điều 5).

Tải trọng và lực cơ học trên các đầu nối điện, khí nén hoặc thủy lực nên được xem xét như một phần của quá trình thiết kế các chi tiết tích hợp của mô đun. Phải đảm bảo những điều sau:

- Tương tác vật lý chính xác của các đầu nối khác nhau về kích thước và về điện;
- Giảm thiểu EMC/ EMI (tương thích điện từ / nhiễu điện từ) giữa các đầu nối khác nhau trong mặt lắp ghép;
- Không rò rỉ chất lỏng hoặc khí trong trường hợp truyền năng lượng chất lỏng qua các đầu nối tích hợp trong mặt lắp ghép.

6.2.2 Kết nối cho bộ nguồn

Các bộ nguồn cung cấp điện hoặc năng lượng cho tất cả các cơ cấu dẫn động. Các nhà sản xuất nên chọn loại bộ nguồn phù hợp, chẳng hạn như điện (AC hoặc DC), khí nén hoặc thủy lực, ví dụ, các nhà sản xuất nên tập trung vào bộ nguồn có điện áp được sử dụng rộng rãi như 5 V, 12 V, 24 V hoặc 48 V.

Các nhà sản xuất phải quy định dòng và công suất tải đầu ra tối đa của bộ nguồn. Các mô đun phải được thiết kế để có mức dự trữ tối thiểu để ghép nối các mô đun bổ sung. Nếu các mô đun có thể được sắp xếp lại tùy ý, thì không thể xác định trước được công suất tối đa có thể được truyền qua một mô đun nhất định.

VÍ DỤ: Mỗi khớp cánh tay cần dòng điện 5 A, vì vậy nếu sáu khớp loại được kết nối nối tiếp trong một cánh tay thì mô đun đầu tiên cần có khả năng truyền 30 A.

Các nguồn điện có thể có pin hoặc các hệ thống lưu trữ năng lượng khác và có thể hoạt động cùng với hệ thống quản lý năng lượng để triển khai các chức năng thông minh.

6.2.3 Các đặc điểm khác cho mô tả mô đun

Đối với mỗi loại mô đun có đặc điểm phần cứng, cần chỉ định các tính năng hoặc dữ liệu quan trọng, ví dụ:

- Các đặc tính động học và động lực học như các thông số hình học, khối lượng, trọng tâm, mô men quán tính và phép biến đổi tọa độ;
- Cấp bảo vệ chống xâm nhập (IP) theo định nghĩa trong IEC 60529.

Nếu có liên quan, cần xác định các đặc điểm liên quan đến môi trường hoạt động sau đây:

- Điều kiện môi trường hoạt động như phạm vi nhiệt độ và độ ẩm;
- Khả năng tương thích sinh học cho các ứng dụng liên quan đến tiếp xúc với con người.

CHÚ THÍCH: Các vấn đề về khả năng tương thích sinh học bao gồm độc tính tế bào, nhạy cảm, kích ứng/phản ứng da, độc tính toàn thân cấp tính, độc tính bán mãn tính, độc tính di truyền, cấy ghép, tương thích máu, độc tính mãn tính, khả năng gây ung thư và khả năng phân hủy sinh học.

Đối với cảm biến và cơ cấu dẫn động, cần mô tả các tính năng cụ thể của mô đun, ví dụ như:

- Độ chính xác và độ phân giải;
- Đối với cảm biến: độ nhạy, phạm vi cảm nhận, đáp ứng tần số, nếu có, và tư thế trong hệ tọa độ nội bộ, nếu có;
- Đối với cơ cấu dẫn động: độ chính xác, công suất/mô men xoắn cực đại và định mức, tốc độ cực đại và định mức và tư thế trong hệ tọa độ nội bộ, nếu có.

7 Đặc điểm phần mềm trong thiết kế mô đun

7.1 Yêu cầu chung

Điều này mô tả các yêu cầu và hướng dẫn được thiết kế để cho phép khả năng tương tác và khả năng tái sử dụng của các mô đun có đặc điểm phần mềm, xem xét các nhu cầu đặc biệt của các mô đun phần mềm có thể được sử dụng trong hệ thống rô bốt dịch vụ. Một mô hình thông tin được sử dụng để đạt được khả năng tương tác và khả năng tái sử dụng. Do đó, với một mô đun cần cung cấp một mô hình thông tin phù hợp. Vì các chi tiết nội bộ của các mô đun như vậy không nằm trong trọng tâm của tiêu chuẩn này, nên điều này tập trung vào các mặt lắp ghép giữa các mô đun, xác định các đầu vào và đầu ra bên ngoài của các mô đun. Vì các mô đun khác nhau có cùng chức năng phải có thể hoán đổi cho nhau, nên các loại dữ liệu đầu vào và đầu ra của các mô đun như vậy cần được xác định bằng cách chỉ định các mô hình truyền thông nào được phép cho các dịch vụ lớp ứng dụng đã sử dụng. Ví dụ về các mô hình truyền thông là mô hình Phát hành/Đăng ký (Pub/Sub); mô hình Máy khách/Máy chủ và mô hình Bảng đen qua bộ nhớ dùng chung (xem Bảng 4). Các mô đun phần mềm cho rô bốt có thể được phát triển dựa trên một khuôn khổ phần mềm trung gian, ví dụ bao gồm ROS, OpenRTM, OPRoS và OROCOS. Các đặc điểm an toàn và bảo mật của các mô đun có đặc điểm phần mềm được trình bày trong Điều 5.

Bảng 4 – Các mô hình giao diện truyền thông tin phần mềm cho các mục đích khác nhau

Số	Loại thông tin	Hỗ trợ trao đổi thông tin	Chú thích
1	Dữ liệu	Công bố / đăng ký kiểu	Dữ liệu có thể được truyền qua một hoặc nhiều kiểu truyền thông Dữ liệu được trao đổi giữa các mô đun, giữa môi trường phát triển tích hợp (hoặc các công cụ) và mô đun
		Khách hàng / mô hình máy chủ	
		Bảng đen (qua bộ nhớ dùng chung)	
2	Gói	Khách hàng / mô hình máy chủ	Các tập tin được trao đổi giữa môi trường phát triển tích hợp (hoặc các công cụ) và mô đun

7.2 Mô hình thông tin

7.2.1 Yêu cầu chung

Các mô đun có đặc điểm phần mềm cho hệ thống rô bốt dịch vụ sẽ cung cấp giao diện phần mềm để truy cập dữ liệu đầu vào/đầu ra, gọi dịch vụ hoặc xử lý sự kiện. Do đó, một thành phần phần mềm cung cấp một số chức năng nội bộ để dữ liệu có thể được sửa đổi thông qua định dạng API hoặc tin nhắn, hoặc dịch vụ từ xa được gọi và kết quả được trả về; và quy trình thích hợp đang hoạt động tại thời điểm xảy ra sự kiện, trong đó dữ liệu từ xa và dịch vụ từ xa được cung cấp bởi các thành phần phần mềm khác.

Ngoài ra, các mô đun có đặc điểm phần mềm có thể truy cập vào các thành phần phần cứng và có thể đọc các cấu hình của các mô đun để khởi tạo và vận hành chúng một cách thích hợp. Điều này có thể thực hiện trực tiếp hoặc thông qua trình điều khiển thiết bị hoặc HAL cho phép các mô đun phần mềm truy cập vào các thành phần phần cứng mà không cần sửa đổi mã của mô đun.

Ngoài ra, các định dạng tin nhắn được cung cấp để kiểm soát và bảo trì phần mềm, chẳng hạn như tải xuống và tải lên các tệp (ví dụ: phần mềm, hồ sơ và các gói ứng dụng) và thực hiện kiểm soát các mô đun phần mềm (ví dụ: bắt đầu, dừng, tạm dừng, tiếp tục, v.v...).

CHÚ THÍCH: Các mô đun phần mềm có thể được xác định bằng cách sử dụng các thông số kỹ thuật hiện có như OMG RoIS (Dịch vụ tương tác bằng rô bốt) cho giao diện dịch vụ hoặc OMG RLS (Dịch vụ định vị bằng rô bốt) để biểu diễn vị trí và hệ tọa độ.

7.2.2 Mô hình cho trao đổi thông tin giữa các mô đun

Mô hình này sẽ được sử dụng để trao đổi thông tin giữa các mô đun, trong đó thông tin bao gồm giá trị của các biến, lệnh gọi dịch vụ, quy trình sự kiện và nội dung của các tệp như mã thực thi của các thành phần phần mềm, hồ sơ hoặc gói. Các biến, dịch vụ và sự kiện được xác định trong các mô đun có đặc điểm phần mềm. Loại biến được phân loại thành các biến tuần hoàn hoặc biến không tuần hoàn và loại dịch vụ được phân loại thành các dịch vụ chặn (hoặc đồng bộ) hoặc các dịch vụ không chặn (hoặc không đồng bộ).

Các giao thức giữa hai hoặc nhiều mô đun có đặc điểm phần mềm không được chỉ định vì có nhiều giao thức truyền thông chuẩn hóa quốc tế và thực tế. Lưu ý rằng truy cập từ xa vào các máy chủ tách biệt được thực hiện bằng định dạng tin nhắn trong điều này do phần mềm trung gian cung cấp. Phần mềm trung gian cũng có thể hỗ trợ trao đổi thông tin giữa các mô đun phần mềm trong máy chủ cục bộ.

CHÚ THÍCH: Ở đây máy chủ cục bộ là mô đun tính toán mà một mô đun phần mềm đang được đăng nhập vào, còn và máy chủ từ xa là mô đun tính toán khác mà phần mềm muốn kết nối thông qua các giao thức truyền thông.

Mô hình trao đổi thông tin giữa các mô đun có các đặc điểm phần mềm sẽ hỗ trợ các nội dung sau:

a) Đọc và ghi dữ liệu;

b) Gọi dịch vụ;

c) Đăng ký và xử lý sự kiện;

d) Chất lượng dịch vụ theo yêu cầu đối với các mục a) đến c). (Ví dụ: giá trị liên quan đến an toàn, các đặc tính thời gian thực, bảo mật).

Thời gian phản hồi trong các trường hợp thời gian thực phải bao gồm tổng thời gian truyền dữ liệu và gọi dịch vụ.

Mô hình phải hỗ trợ ít nhất một trong các phương pháp ưu tiên sau đây để đọc và ghi dữ liệu trong các bản sao của các mô đun phần mềm khác:

- Yêu cầu có phản hồi, yêu cầu không có phản hồi;

- Đăng ký/ xuất bản;
- Bảng đen (qua bộ nhớ dùng chung).

Các nhà sản xuất có thể áp dụng các phương pháp khác khi chúng nổi trội, nhưng các yêu cầu về khả năng tương tác phải được cung cấp trong mẫu mô đun.

Nhà sản xuất mô đun phải thiết kế định dạng tin nhắn để trao đổi thông tin nhằm đáp ứng các điều sau:

- Hỗ trợ phần mềm trung gian.
- Hỗ trợ các quy tắc mã hóa/giải mã để trao đổi thông tin giữa hai hoặc nhiều phần mềm trung gian.
- Thông tin hỗ trợ cho điều này có thể được tìm thấy trong 7.2.3, 7.2.4 và 7.4.2.

7.2.3 Mô hình truy cập vào các thuộc tính và quyền truy cập

Một mô đun có đặc điểm phần mềm sẽ sử dụng các giá trị thuộc tính của nó để thực thi đúng và thiết lập các giá trị để khởi tạo nó. Mô đun phải có các thuộc tính sau:

a) Thông tin của nhà sản xuất cho mô đun;

b) Môi trường thực thi, ví dụ, loại hệ điều hành, loại thực thi (định kỳ, không thường xuyên, không theo thời gian thực, theo thời gian thực, v.v.), thời gian thực thi nếu loại thực thi là định kỳ, v.v...;

c) Chế độ truyền thông được hỗ trợ (ví dụ: xuất bản/đăng ký, máy khách/máy chủ, bảng đen, v.v...);

d) Mức độ bảo mật (tính bảo mật, tính toàn vẹn, xác thực, số bit trong khóa);

e) Thông tin liên quan đến an toàn (ví dụ: ghi nhãn bắt buộc PL hoặc SIL).

Ngoài ra, mô đun phải có các thuộc tính sau:

f) Các lệnh gọi dịch vụ (chặn hoặc không chặn) được cung cấp bên ngoài;

g) Thông tin được cung cấp bên ngoài;

h) Các giá trị khởi tạo cần thiết để thực thi đúng, và

i) Các yêu cầu về phần mềm và phần cứng phù hợp để đảm bảo hoạt động và an toàn của mô đun.

Nếu một mô đun yêu cầu một trình tự các sự kiện và/hoặc các lệnh cụ thể để được khởi tạo đúng cách hoặc nếu các mô đun yêu cầu một trình tự cụ thể các sự kiện bật, thì một mô đun như mô đun giám sát sẽ quản lý các trình tự đó.

VÍ DỤ 1: Tất cả các mô đun bánh xe phải được đưa vào hoạt động chính xác trước khi các bộ phận phía trên của hệ thống rô bốt được đưa vào hoạt động.

VÍ DỤ 2: Một mô đun cảm biến laser hoặc một mô đun camera phải được khởi tạo và hoạt động trước khi có thể sử dụng để điều hướng an toàn.

Các trình tự này ở cấp độ rô bốt dịch vụ cần được triển khai và cấu hình bởi hệ thống tích hợp và có thể được kiểm soát bởi một mô đun như mô đun giám sát.

Một mô đun có các đặc điểm phần mềm sẽ cung cấp các chức năng để đọc hồ sơ, đặt các thuộc tính từ hồ sơ vào các thành phần phần mềm và ghi các thuộc tính đã sửa đổi vào hồ sơ, nơi các thuộc tính được chỉ định. Mô đun sẽ sử dụng các chức năng do mô hình xác định để đọc hồ sơ nhằm khởi tạo các thành phần phần mềm, cung cấp các dịch vụ của các thành phần phần mềm và truy cập dữ liệu được lưu trữ.

Mô đun này sẽ hỗ trợ các chức năng sau:

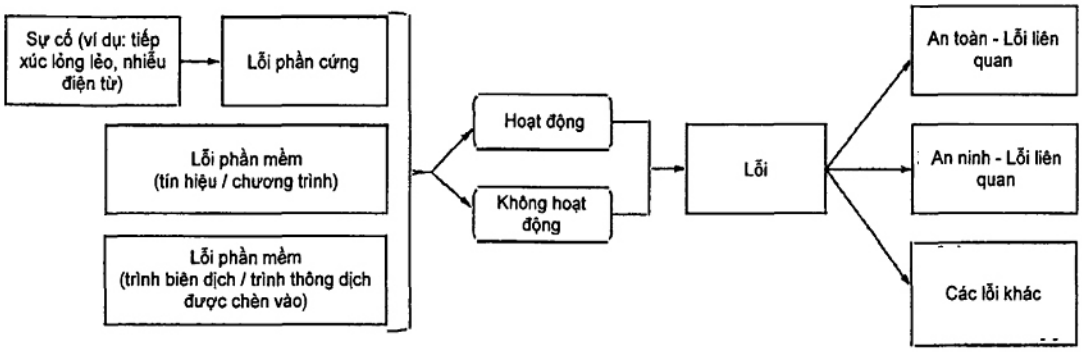
- Đặt (các) giá trị thuộc tính;
- Lấy (các) giá trị thuộc tính.

7.2.4 Mô hình xử lý lỗi và phục hồi

Lỗi trong các mô đun có thể khiến rô bốt dịch vụ trục trặc hoặc không hoạt động bình thường. Những lỗi này có thể khiến dịch vụ rô bốt gặp tình huống nguy hiểm. Để tránh những tình huống như vậy, lỗi phải được phát hiện càng sớm càng tốt và phải đảm bảo chúng được khắc phục và các tình huống nguy hiểm được ngăn ngừa.

CHÚ THÍCH 1: Lỗi là biểu hiện rõ ràng của sai sót.

Các lỗi phải được phân loại thành lỗi liên quan đến an toàn và lỗi không liên quan đến an toàn, như thể hiện trên Hình 4; điều này có thể được thực hiện thông qua người quản lý an toàn/bảo mật. Lưu ý rằng lỗi liên quan đến an toàn có thể xảy ra lỗi không liên quan đến an toàn, tùy thuộc vào ứng dụng và môi trường hoạt động.



Hình 4 – Lỗi liên quan và không liên quan đến an toàn

Một mô đun có các đặc điểm phần mềm xử lý lỗi phải hỗ trợ các chức năng sau đây để xử lý lỗi và phục hồi sau các tình huống lỗi:

- Gửi và nhận trạng thái lỗi và dữ liệu phục hồi lỗi đến/từ các mô đun bên ngoài (Hình 6) như mô đun quản lý an toàn (xem 7.4);
- Phân loại lỗi thành lỗi liên quan đến an toàn, lỗi liên quan đến bảo mật và các lỗi khác được chỉ định bởi ứng dụng;

CHÚ THÍCH 2: Lỗi không liên quan đến an toàn được bao gồm trong các lỗi khác.

- Hỗ trợ chu trình thực hiện (Hình 6) để đảm bảo an toàn (xem 7.3);
- Cung cấp các phương pháp xử lý lỗi không xác định.

Các nhà thiết kế mô đun nên xác định các phản ứng phù hợp tùy theo các loại lỗi được phân loại. Đối với các lỗi liên quan đến an toàn, có thể cần phải truyền lỗi ngay lập tức đến cấp hệ thống (ví dụ: mô đun quản lý an toàn). Ngoài ra, các lỗi liên quan đến bảo mật có thể yêu cầu xử lý ở cấp hệ thống (ví dụ: mô đun quản lý bảo mật). Các lỗi khác được xử lý ở cấp thấp hơn, nếu có thể (ví dụ: trong chính mô đun).

Các mô đun được chỉ định để xác định và xử lý lỗi phải có đủ độ tin cậy. Mức hiệu quả của mô đun như vậy phải cao ít nhất bằng mức hiệu quả yêu cầu của bất kỳ chức năng an toàn nào liên quan đến các lỗi đã xử lý.

Nếu có hai hoặc nhiều mô đun bên ngoài có thể xử lý cùng một lỗi, các mô đun đó phải có mức độ ưu tiên được đặt để gửi phản hồi/lệnh đến các lỗi.

7.2.5 Hoạt động tương tác của các mô đun phần mềm

Các mô đun phải có khả năng truyền thông và tương tác với các mô đun do các nhà sản xuất khác nhau phát triển.

Các mục sau đây sẽ được cung cấp trong bảng dữ liệu mô đun để đảm bảo khả năng tương tác hiệu quả giữa các mô đun rô bốt dịch vụ:

a) Thông tin được trao đổi giữa các mô đun khi cần (xem 7.2.2);

b) Thông tin để quản lý mô đun (xem 7.4.2);

c) Thông tin được sử dụng trong hồ sơ thuộc tính cho mô đun (xem 7.2.3), và

d) Thông tin để xử lý lỗi và phục hồi (xem 7.2.4).

Mục sau đây cần được cung cấp để đảm bảo khả năng tương tác và khả năng tái sử dụng hiệu quả giữa các mô đun kiểu rô bốt dịch vụ:

e) Mô hình thông tin đã xác định giữa các mô đun và phần mềm trung gian (xem 7.2.2).

Mục sau đây có thể được cung cấp để đảm bảo khả năng tương tác và khả năng tái sử dụng hiệu quả giữa các mô đun kiểu rô bốt dịch vụ:

f) Mô hình được xác định cho lớp trừu tượng phần cứng hoặc trình điều khiển thiết bị.

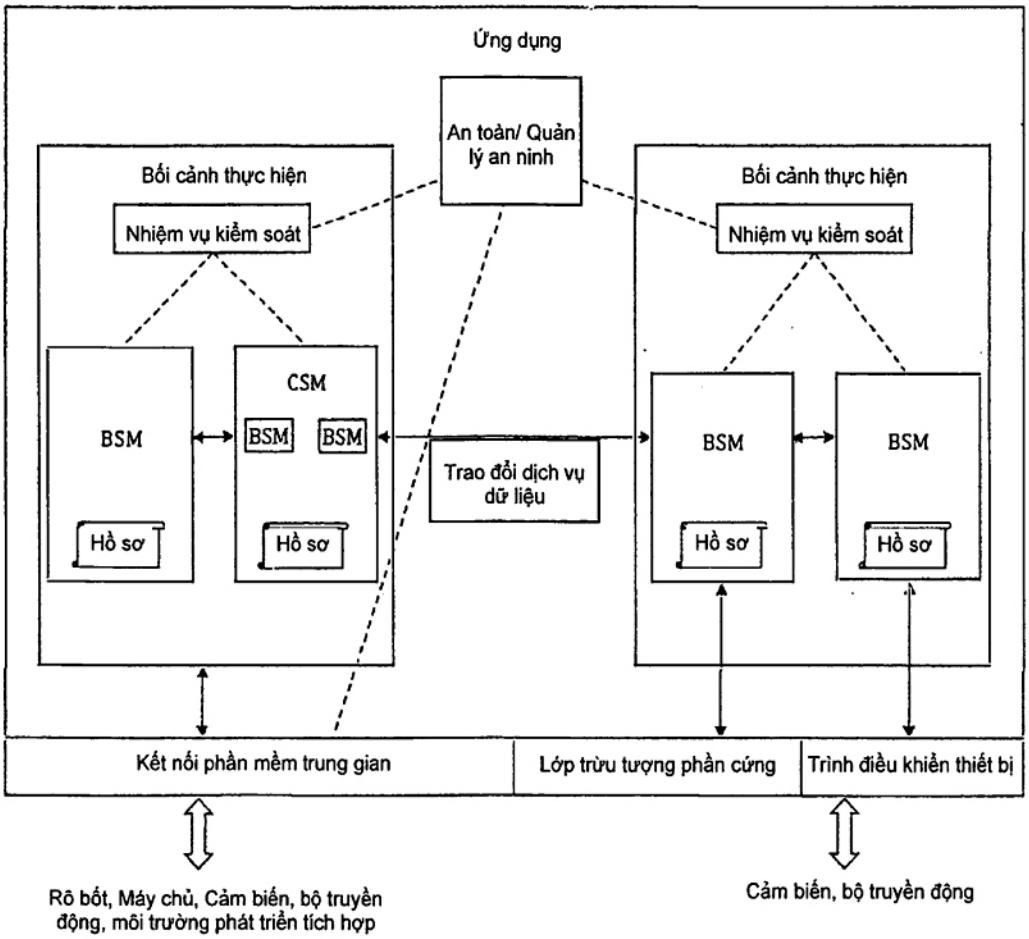
CHÚ THÍCH: Hồ sơ thuộc tính được lưu trữ trong kho lưu trữ hồ sơ.

7.3 Mô hình kiến trúc cho các mô đun phần mềm

7.3.1 Yêu cầu chung

Mô hình kiến trúc cho các mô đun phần mềm phải bao gồm ngữ cảnh thực thi và các tác vụ kiểm soát. Mô hình được sử dụng cho an toàn và bảo mật phải bao gồm một trình quản lý an toàn và một trình quản lý bảo mật. Các mô đun phần mềm và mối quan hệ giữa chúng được minh họa trên Hình 5. Hình này

cho thấy ví dụ về một số mô đun phần mềm được kết nối với nhau. Một số mô đun là các mô đun phần mềm cơ bản, trong khi những mô đun khác là mô đun tổng hợp vì chúng có thể được phân tách thành các mô đun nhỏ hơn. Hai ngữ cảnh thực thi được hiển thị, về cơ bản là các luồng điều khiển bị cô lập có thể được lưu trữ trên các bộ xử lý khác nhau (hoặc không). Một trình quản lý an toàn và bảo mật riêng biệt sẽ quan sát hành vi của mô đun như một tổng thể và giao tiếp với các mô đun khác diễn ra thông qua giao diện trừu tượng hóa phần cứng/trình điều khiển thiết bị và phần mềm trung gian giao tiếp. Các trình quản lý an toàn hoặc bảo mật được triển khai riêng biệt dưới dạng các mô đun độc lập. Trình quản lý an toàn sẽ chỉ nhận dữ liệu có liên quan từ các mô đun phần mềm liên quan đến an toàn.



Hình 5 – Kiến trúc khung chuẩn của phần mềm cho rô bốt dịch vụ hệ mô đun

Kho lưu trữ hồ sơ.quản lý các hồ sơ được các mô đun sử dụng.

Bối cảnh thực thi là phần tử bao gồm một hoặc nhiều mô đun phần mềm và một tác vụ điều khiển. Tác vụ điều khiển phối hợp các mô đun phần mềm trong bối cảnh thực thi và quản lý các ràng buộc thời gian thực của chúng nếu có.

Ứng dụng là phần tử điều khiển hệ thống rô bốt theo nhu cầu của người dùng và bao gồm một hoặc nhiều bối cảnh thực thi. Ứng dụng sử dụng gói ứng dụng, bao gồm các mô đun phần mềm, các giá trị và các bước để khởi tạo và các tài nguyên liên quan để thực thi ứng dụng.

Cơ chế trừu tượng hóa, chẳng hạn như giao diện trừu tượng hóa phần cứng, giúp các mô đun phần mềm truy cập phần cứng độc lập với các đặc điểm phụ thuộc vào phần cứng. Các mô đun phần mềm có thể đọc/ghi dữ liệu từ/vào phần cứng tương ứng thông qua cơ chế trừu tượng hóa, cho phép các mô đun phần mềm có tính linh động. Các mô đun gồm cả các mô đun phần mềm truy cập các bộ phận cảm biến/ kích hoạt bằng cơ chế trừu tượng hóa để lấy dữ liệu từ các thiết bị và truyền dữ liệu cho các mô đun khác.

Phần mềm trung gian truyền thông trao quyền cho các mô đun phần mềm và thành phần phần mềm trao đổi thông tin. Phần mềm trung gian có thể quản lý các tệp liên quan đến các mô đun phần mềm, thành phần và ứng dụng và tải lên/tải xuống các tệp cần thiết có liên quan từ/đến máy chủ và/hoặc rô bốt. Phần mềm trung gian truyền thông có thể được triển khai trong bối cảnh thực thi theo mô hình trao đổi thông tin được hiển thị trong Bảng 4. Lưu ý rằng phần mềm trung gian không được định nghĩa trong tiêu chuẩn này.

Người quản lý bảo mật sẽ quản lý các sự cố bảo mật đã xảy ra trong cả các mô đun phần mềm cũng như ở các phần khác khi cần. Ví dụ, người quản lý bảo mật có thể giám sát và kiểm soát các rủi ro như truy cập của người dùng trái phép.

Người quản lý an toàn sẽ quản lý các sự cố liên quan đến an toàn xảy ra trong tất cả các mô đun phần mềm cũng như các phần khác khi cần. Ví dụ, người quản lý an toàn sẽ giám sát trạng thái thực thi của các mô đun phần mềm, phát hiện xem có vi phạm giới hạn nào không hoặc rô bốt có đang rơi vào tình huống nguy hiểm không và nếu có thì đưa rô bốt về trạng thái an toàn.

7.3.2 Các yêu cầu đối với mô đun phần mềm

Các mô đun có đặc điểm phần mềm bao gồm mã thực thi và một hồ sơ, trong đó hồ sơ lưu trữ các giá trị của các thuộc tính mô đun để hỗ trợ việc thực thi đúng của mô đun.

VÍ DỤ 1: Ví dụ về thuộc tính mô đun: số phiên bản, loại hệ điều hành, phương thức dịch vụ được cung cấp, loại thực thi như thực thi định kỳ, thực thi không thường xuyên và không theo thời gian thực và các thuộc tính mô đun liên quan đến phần cứng. Ví dụ về giá trị của thuộc tính mô đun: giá trị để khởi tạo, giá trị cần thiết để thực thi mô đun phần mềm như loại hệ điều hành, giao thức truyền thông được hỗ trợ, loại dịch vụ và loại sự kiện được hỗ trợ.

VÍ DỤ 2: Ví dụ về mô đun phần mềm cơ bản: mô đun tính toán khoảng cách, đọc dữ liệu khoảng cách đã đo qua giao diện trừu tượng phần cứng từ phần cứng phù hợp (như cảm biến siêu âm, cảm biến hồng ngoại hoặc cảm biến laser), chuyển đổi dữ liệu thành dữ liệu có định dạng chuẩn chính xác và gửi dữ liệu đã chuyển đổi đến các mô đun phần mềm khác. Một ví dụ về các mô đun phức tạp hơn sẽ là mô đun đo khoảng cách âm thanh nổi hoặc mô đun phát hiện đối tượng chạy trên luồng hình ảnh nhận được từ mô đun cảm biến (camera).

VÍ DỤ 3: Một ví dụ điển hình của mô đun phần mềm tổng hợp là mô đun phần mềm thao tác bao gồm các mô đun phần mềm cơ bản như mô đun điều khiển cơ cấu dẫn động, mô đun đồng bộ trục, mô đun động học ngược và mô đun lập kế hoạch đường dẫn, được mô tả như các ví dụ trong Phụ lục B.

Mô đun phần mềm phải được thiết kế để đáp ứng các yêu cầu sau:

a) Hỗ trợ trao đổi thông tin với các mô đun khác thông qua mô hình thông tin xác định (xem 7.2.2);

b) Hỗ trợ Chất lượng dịch vụ (ví dụ: đặc điểm thời gian thực) nếu được quy định;

c) Có mã định danh duy nhất và lấy giá trị của các thuộc tính mô đun cần thiết cho hoạt động và khả năng tương tác phù hợp;

VÍ DỤ 4: Thông tin về khả năng tái sử dụng, khả năng tương tác và khả năng tổ hợp của các ví dụ về mô đun phần mềm là loại hệ điều hành, loại giao thức truyền thông, loại giao diện cho dịch vụ và loại dữ liệu được sử dụng.

d) Tạo một hoặc nhiều phiên bản có mã định danh duy nhất cho từng mô đun phần mềm trong ứng dụng;

e) Được kiểm soát bởi tác vụ kiểm soát quản lý chu trình thực hiện của nó như thể hiện trên Hình 6;

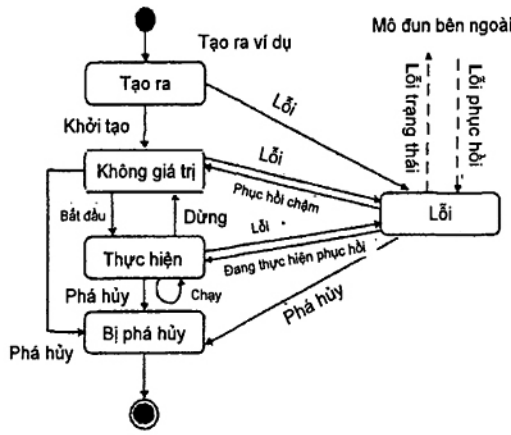
f) Hỗ trợ tính an toàn ở cấp độ mô đun tùy thuộc vào các loại lỗi có khả năng xảy ra trong mô đun phần mềm, hồ sơ thuộc tính mô đun của nó và kết nối của nó với các mô đun khác;

g) Hỗ trợ bảo mật ở cấp độ mô đun nếu mô đun có thể truy cập các mô đun bên ngoài;

h) Có hồ sơ bao gồm các giá trị của các thuộc tính mô đun xác định trong 7.2.3;

i) Hỗ trợ tính độc lập với nền tảng phần mềm.

CHÚ THÍCH 1: Tiêu chuẩn này cho phép các mô đun phần mềm hoặc các thành phần phần mềm trong các mô đun được thực thi thông qua nhiều ngôn ngữ lập trình khác nhau, trên các hệ điều hành khác nhau, với các định dạng tệp tài liệu hoặc cơ sở dữ liệu khác nhau.



Hình 6 – Chu trình thực hiện của mô đun phần mềm bao gồm xử lý lỗi

Các mô đun phần mềm phải tuân thủ chu trình thực hiện được thể hiện trong Hình 6, chu trình này thực hiện các hành vi sau: Khi một mô đun phần mềm được tạo, mô đun sẽ chuyển sang trạng thái 'đã tạo'. Sự kiện 'khởi tạo' xảy ra khi mô đun phần mềm được khởi tạo. Sự kiện 'khởi động' xảy ra khi quá trình thực thi mô đun phần mềm được bắt đầu. Sự kiện 'dừng' xảy ra khi quá trình thực thi mô đun phần mềm bị dừng lại và sự kiện 'chạy' xảy ra tại mỗi khoảng thời gian nhất định. Sự kiện 'hủy' xảy ra khi mô đun phần mềm được rút khỏi bộ nhớ sau khi hoàn tất quá trình thực thi hoặc bị xóa. Sự kiện 'lỗi' được tạo khi lỗi xảy ra ở bất kỳ trạng thái nào của mô đun phần mềm. Sự kiện 'phục hồi khi rỗi' và 'phục hồi khi thực thi' được tạo để khôi phục lỗi ở các trạng thái tương ứng là đã tạo, đang chờ hoặc đang thực thi. Đặc biệt, 2 loại sự kiện 'phục hồi khi rỗi' và 'phục hồi khi thực thi' được thiết kế cho hoạt động khôi phục

lỗi. Lưu ý rằng mỗi sự kiện sẽ khiến hàm liên quan được gọi; định kỳ, một mô đun thời gian thực thực hiện các hàm liên quan bằng cách sử dụng sự kiện 'chạy'.

CHÚ THÍCH 2: Khi một mô đun phần mềm liên quan đến an toàn ở trạng thái 'lỗi', các lỗi liên quan đến an toàn sẽ được gửi đến các mô đun bên ngoài khác để xử lý các lỗi và trả về các giá trị khôi phục phù hợp. Một ví dụ về mô đun bên ngoài có thể là mô đun phần mềm hoặc mô đun có thể xử lý lỗi để tránh rơi vào các tình huống nguy hiểm. Ví dụ điển hình là trình quản lý an toàn như được hiển thị trên hình 5.

Đối với các lỗi được xử lý trong phần liên quan đến an toàn của hệ thống điều khiển, các quy trình khôi phục lỗi (đặc biệt là 'khôi phục khi thực thi') phải tuân theo ISO 12100 và ISO 14118 để ngăn ngừa các mối nguy hiểm do khởi động bất ngờ.

7.4 Các yêu cầu liên quan đến an toàn/bảo mật cho mô đun có các đặc điểm phần mềm

7.4.1 Yêu cầu chung

Các mô đun phần mềm liên quan đến an toàn sẽ được thiết kế dựa trên Điều 5. Tính bảo mật của các mô đun đó liên quan đến an ninh mạng và được mô tả từ 5.2 đến 5.10. Điều này mô tả mô đun quản lý an toàn/bảo mật (xem Hình 5) để quản lý các vấn đề an toàn/bảo mật không thể xử lý bên trong mô đun. Lưu ý rằng mô đun quản lý an toàn/bảo mật có thể được triển khai dưới dạng một mô đun tích hợp hoặc hai mô đun độc lập, cụ thể là một mô đun an toàn và một mô đun bảo mật. Các mô đun cũng có thể được triển khai dưới dạng kiến trúc dự phòng để đáp ứng PL/ SIL liên quan.

Mô đun quản lý bảo mật là mô đun dùng để quản lý bảo mật của rô bốt và các mô đun của nó, có thể thiết lập hoặc triển khai chính sách bảo mật để quản lý các phản hồi về các vấn đề bảo mật. Lưu ý rằng các vấn đề bảo mật có thể xảy ra khi một mô đun trao đổi dữ liệu, chẳng hạn như giá trị và tệp, với các mô đun bên ngoài hoặc khi người dùng trái phép có quyền truy cập vào rô bốt mà không có quyền hợp lệ, v.v... Khi một mô đun trao đổi dữ liệu với một mô đun bên ngoài hoặc bên trong, dữ liệu tương ứng phải không được nghe lén hoặc sửa đổi, điều này được thực hiện bằng các biện pháp bảo mật mạng thích hợp như mã hóa và xác thực. Khi các chương trình hoặc cấu hình được tải xuống hoặc lệnh điều khiển được nhận từ người gửi tin nhắn bên ngoài rô bốt, việc ủy quyền của người gửi tin nhắn sẽ được giám sát và kiểm soát bởi mô đun quản lý an toàn/ bảo mật.

7.4.2 Tương tác với các mô đun quản lý an toàn/ bảo mật

Các mô đun liên quan đến an toàn sẽ cung cấp thông tin sau cho mô đun quản lý an toàn để xử lý an toàn cho phần mềm hệ mô đun:

- Thông tin lỗi do môđun cung cấp;
- Thông tin khôi phục lỗi mà mô đun nhận được.

Mô đun quản lý an toàn sẽ xử lý toàn diện thông tin lỗi nhận được từ mỗi mô đun liên quan đến an toàn và cung cấp thông tin để thực hiện dừng hoặc hoạt động an toàn cho mỗi mô đun. Hoạt động dừng có thể được chia thành dừng hoạt động của rô bốt và dừng hoạt động của các mô đun liên quan đến một

sự kiện cụ thể. Việc dừng và khởi động lại phải tuân theo các tiêu chuẩn an toàn hiện hành như TCVN 7383 (ISO 12100) (về các phần chung) và IEC 60204-1 (để dừng) và ISO 14118 (để khởi động).

Trong khi một mô đun trao đổi dữ liệu với một mô đun bên ngoài hoặc bên trong bằng các phương pháp giao tiếp, tính toàn vẹn và xác thực phải được xác minh. Đặc biệt, tính toàn vẹn và xác thực phải được xác minh khi thực hiện truyền thông giữa các công cụ phát triển/giám sát bên ngoài và máy chủ. Trong trường hợp sử dụng bus trường không hỗ trợ bảo mật, bảo mật vật lý phải đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vật lý vào bus trường. Ngoài ra, an ninh mạng phải đảm bảo việc truyền tải các dữ liệu sau đây nếu cần thiết:

- Gói, mô đun phần mềm và hồ sơ của chúng;
- Kiểm soát trạng thái thực thi của từng mô đun phần mềm;
- Dữ liệu đầu vào và đầu ra của các mô đun.

Trình quản lý bảo mật phải được vận hành kết hợp với trình quản lý an toàn để có thể vận hành theo chính sách riêng của rô bốt ngay cả khi rô bốt không giao tiếp với bên ngoài do các cuộc tấn công từ chối dịch vụ hoặc các vấn đề tương tự khác. Do đó, mô đun trình quản lý an toàn/bảo mật phải có các chức năng sau:

- Trình quản lý bảo mật gửi thông tin liên quan đến an toàn cho trình quản lý an toàn nếu trình quản lý bảo mật phát hiện ra các vấn đề bảo mật liên quan đến an toàn.
- Trình quản lý an toàn kiểm soát các mô đun theo chính sách an toàn đã chỉ định, được thiết lập trước.

8 Thông tin cho sử dụng

8.1 Yêu cầu chung

Các nhà sản xuất mô đun phải cung cấp đủ tài liệu kèm theo mô đun của họ, để các bên thứ ba có thể sử dụng mô đun (chẳng hạn như tích hợp vào hệ thống lớn hơn hoặc tạo các mô đun khác tương tác với mô đun được cung cấp) dựa trên tài liệu được cung cấp. Các nhà sản xuất mô đun phải cung cấp danh sách các tiêu chuẩn mà mô đun tuân thủ và cung cấp tất cả các tài liệu theo yêu cầu của các tiêu chuẩn đó. Điều khoản này bao gồm các yêu cầu về tài liệu bổ sung để hỗ trợ hệ mô đun.

Bên tích hợp rô bốt dịch vụ phải hoàn thiện thông tin để sử dụng cho hệ thống rô bốt dịch vụ với tất cả thông tin cần thiết cho người dùng hệ thống. Điều này phải bao gồm những nội dung sau:

- Cung cấp hướng dẫn sử dụng cho toàn bộ hệ thống.
- Thêm hoặc thay thế các biển cảnh báo, các dấu hiệu và chỉ dẫn khác trên rô bốt.
- Cung cấp sơ đồ hệ thống chỉ ra tất cả các mô đun mà rô bốt được chế tạo cùng các kết nối của chúng.

Các nhà tích hợp rô bốt dịch vụ phải cung cấp thông tin cho người dùng hệ thống rô bốt dịch vụ về việc sử dụng từng mô đun trong rô bốt.

Các nhà tích hợp rô bốt dịch vụ phải nêu trong tài liệu của họ, những sửa đổi nào (ví dụ: trao đổi mô đun) của hệ thống rô bốt dịch vụ được người dùng cho phép.

Thông tin sử dụng bao gồm thông tin về việc sử dụng đúng mô đun để thực hiện các nhiệm vụ dự định với mô đun. Người dùng có thể là, nhưng không giới hạn, nhà sản xuất rô bốt, nhà thiết kế mô đun, người thử nghiệm mô đun hoặc tham gia bảo trì mô đun.

Các dấu hiệu, ký hiệu và cảnh báo bằng văn bản phải dễ hiểu và rõ ràng để cung cấp chi tiết về mô đun. Đối với các mô đun cơ bản, thông tin phải bao gồm loại mô đun (đầu vào, tính toán, xử lý, cơ sở hạ tầng và đầu ra). Đối với các mô đun tổng hợp, cần cung cấp đủ thông tin chi tiết về các mô đun cơ bản và thường dùng khác nhau.

Các biển báo dạng biểu tượng có thể được sử dụng để cảnh báo rõ ràng hoặc để minh họa môi trường hoạt động. Tất cả các dấu hiệu in phải dễ đọc và bền. Dấu hiệu liên quan đến an toàn phải tuân theo các yêu cầu và hướng dẫn tương ứng từ các tiêu chuẩn an toàn hiện hành. Nên ưu tiên sử dụng biểu tượng hơn là các cảnh báo bằng văn bản, nếu có thể, để việc sử dụng mô đun dễ dàng hơn ở các khu vực khác nhau.

Nhà sản xuất mô đun phải cung cấp cả phiên bản in và điện tử của thông tin cho sử dụng, có lưu ý đến các yếu tố con người và khả năng sử dụng của các tài liệu.

Mô tả về mô đun phải sử dụng Mẫu mô đun rôbốt được chỉ định trong Phụ lục A. Thông tin bổ sung không có trong mẫu, nếu có, phải được trình bày ở định dạng tương tự.

Khi có chỉ dẫn, chúng phải được mô tả bằng các dấu hiệu trên mô đun hoặc trong tài liệu của mô đun.

8.2 Dấu hiệu hoặc chỉ dẫn

Phải có các dấu hiệu trên mô đun và dùng các mẫu dễ nhận biết từ bên ngoài mô đun.Dấu hiệu phải chi tiết khi cần thiết nhưng ít nhất cũng phải bao gồm tên hoặc dấu hiệu tương đương của nhà cung cấp mô đun, số kiểu hoặc loại của mô đun và các dấu hiệu để sử dụng bình thường, bao gồm tất cả các dấu hiệu hoặc chỉ dẫn theo yêu cầu của các tiêu chuẩn an toàn đã công bố và có liên quan.

Đối với mô đun có các đặc điểm phần cứng, dấu hiệu phải dễ nhìn, dễ đọc, không thể xóa được và ít nhất phải bao gồm các thông tin sau:

- Tên nhà sản xuất
- Số sê-ri
- Dấu hiệu chứng nhận về an toàn và bảo mật, nếu có

Các mô đun phần mềm ít nhất phải chứa các thông tin sau đây trong tài liệu của chúng, chẳng hạn như hướng dẫn sử dụng hoặc tệp văn bản trên phương tiện lưu trữ điện tử được sử dụng để phân phối mô đun phần mềm:

- Tên nhà sản xuất
- Loại mô đun phần mềm và số phiên bản

- Loại hệ điều hành
- Số sê-ri

8.3 Thông tin cho người dùng

Thông tin cho người dùng của mô đun phải được cung cấp để sử dụng đúng mục đích và có chủ đích.

Thông tin cho người dùng phải bao gồm những nội dung sau:

a) Mô tả chi tiết về mô đun

- Hướng dẫn sử dụng mô đun
- Mô tả ngắn gọn về các mô đun cơ bản và/hoặc các mô đun tổng hợp có trong mô đun
  - Mô tả về mô đun có đặc điểm phần cứng
    - Tên và thông tin liên hệ của nhà sản xuất, quốc gia sản xuất
    - Loại mô đun và số phiên bản
    - Các tính năng kết nối liên thông có trong mô đun (hướng của đầu nối, chỉ định chân, v.v....)
    - Số sê-ri, nếu cần
    - Giá trị định mức cho nguồn cung cấp (ví dụ: nguồn điện áp hoặc phạm vi định mức tính bằng vôn (DC/AC), tần số định mức nếu cần, áp suất khí nén, v.v...)
    - Công suất định mức tính bằng watt hoặc dòng điện định mức tính bằng ampe
    - Loại giao tiếp nếu sử dụng
    - Dấu chứng nhận an toàn, nếu có
    - Các tính năng bảo mật, nếu có
    - Khối lượng (tính bằng kg) và kích thước 3D (tính bằng mm)
  - Mô tả cho mô đun có đặc điểm phần mềm
    - Tên nhà sản xuất và thông tin liên hệ, quốc gia của nhà sản xuất
    - Loại mô đun phần mềm và số phiên bản
    - Loại hệ điều hành và thông tin chi tiết
  - Số sê-ri, nếu cần
  - Danh sách kiểm tra để sử dụng mô đun. Ví dụ: loại mô đun phù hợp cho ghép nối, mô đun phần cứng được hỗ trợ (ví dụ: để ghép nối cơ khí/điện phù hợp) hoặc mô đun phần mềm tương thích
  - Môi trường hoạt động cho các mô đun
  - Phương pháp cài đặt cho các mô đun phần mềm, nếu có

- Chi tiết để kết nối với các mô đun khác
- Danh sách các nguyên tắc như tại Điều 4 kèm theo mô đun

b) Các ứng dụng có trường hợp sử dụng phù hợp, bao gồm thông tin liên quan đến an toàn và bảo mật của chúng, nếu có

c) Chi tiết để thiết lập và điều chỉnh các giá trị thuộc tính mô đun

d) Danh sách các mô đun cơ bản có thể thay thế và các mô đun tổng hợp, nếu có

e) Danh sách các sai sót hoặc lỗi đã biết

f) Phương pháp sạc pin, nếu có liên quan

g) Thông tin để nâng hạ và vận chuyển mô đun với thông tin chi tiết về các điểm cầm nắm và treo móc

h) Danh sách các vật tư tiêu hao và chu kỳ bảo dưỡng của chúng

Thông tin liên quan đến an toàn cần thiết để duy trì chức năng an toàn khi tích hợp các mô đun nên được cung cấp, nếu phù hợp, theo định dạng có cấu trúc và được định nghĩa rõ ràng.

8.4 Thông tin cho bảo dưỡng

Thông tin để bảo dưỡng phải bao gồm hướng dẫn để duy trì hoạt động chính xác của mô đun với các chi tiết về những nhiệm vụ có yêu cầu kiến thức kỹ thuật cụ thể hoặc kỹ năng chuyên môn, do đó cần được thực hiện bởi những người thích hợp (ví dụ: nhân viên bảo trì, chuyên gia, v.v...).

Thông tin về bảo dưỡng phải bao gồm những thông tin sau:

a) Mô tả chi tiết về mô đun và các yêu cầu bảo trì

b) Thông tin về môi trường vận hành thực tế khi thích hợp (ví dụ: cường độ sáng cho mô đun thị giác, chất gây ô nhiễm trong khí quyển, nhiệt độ khắc nghiệt, v.v...)

c) Thông tin (nếu có) về:

- Hướng dẫn thiết lập, lịch bảo trì và các thông số vận hành danh nghĩa
- Trình tự các hoạt động để kiểm tra bảo trì
- Tần suất kiểm tra
- Tần suất và phương pháp kiểm tra chức năng của các mô đun
- Hướng dẫn về việc điều chỉnh, bảo trì và sửa chữa khi cần
- Danh sách phụ tùng thay thế được khuyến nghị cho các mô đun có đặc điểm phần cứng
- Danh sách các công cụ cần thiết và được cung cấp

d) Sơ đồ cơ khí chi tiết và sơ đồ khối điện

e) Danh sách các lỗi hoặc sai sót đã biết và mô tả của chúng

f) Danh sách các vật tư tiêu hao và chu kỳ bảo trì của chúng

Phụ lục A

(Tham khảo)

Mẫu mô tả mô đun rô bốt

A.1 Mẫu mô tả chung

Nhiều mô đun khác nhau được giới thiệu trong tiêu chuẩn này và vì mục đích thống nhất, các mô tả mô đun phải tuân theo một mẫu chung để có thể phát triển một định dạng chuẩn. Bảng A.1 thể hiện một Mẫu mô tả mô đun rô bốt. Trong Bảng A.1, văn bản in nghiêng cho biết các thông tin cần đưa vào từng phần của mẫu. Các nhà sản xuất nên sử dụng mẫu này để mô tả chi tiết các mô đun của họ. Thông tin bổ sung cũng có thể được cung cấp khi thích hợp.

Bảng A.1 – Diễn giải về Mẫu mô tả mô đun rô bốt tiêu chuẩn

Tên mô đun: *Tên bằng ngôn ngữ tự nhiên của một mô đun hoặc lớp mô đun cụ thể.*
Mô tả: *Tổng quan về mô đun, mô đun là gì, chức năng của mô đun và cách sử dụng mô đun trong các tình huống ứng dụng dự kiến: mô tả các tình huống ứng dụng của mô đun rô bốt để có thể thực hiện các bài kiểm tra xác nhận nếu cần.*
Nhà sản xuất: *Thông tin liên hệ của nhà phát triển mô đun. Thông tin này có thể bao gồm thông tin chi tiết về nhà thiết kế, nhà sản xuất hoặc tổ chức nhà cung cấp.*
Mã nhận dạng mô đun (ID): *Số tham chiếu sản phẩm duy nhất của nhà sản xuất cho mô đun.*
Ví dụ: *Các ví dụ về trường hợp sử dụng điển hình của mô đun.*
Các đặc điểm phần cứng: *Chi tiết tóm tắt về các đặc điểm phần cứng, xem Điều 6 (qua các ví dụ nếu có thể).*
Các đặc điểm phần mềm: *Chi tiết tóm tắt về các đặc điểm phần mềm, xem Điều 7 (qua các ví dụ nếu có thể).*
Thuộc tính của mô đun: *Danh sách các thuộc tính mô đun (xem Điều 6 và 7).*
Đầu vào: *Danh sách các đầu vào của mô đun.*
Đầu ra: *Danh sách các đầu ra của mô đun.*
Chức năng/Tính năng: *Mô tả cách mô đun tiếp nhận đầu vào và xử lý chúng để xác định đầu ra của nó. Nên sử dụng các sơ đồ phù hợp (ví dụ sử dụng các phương pháp đường thẳng, đường tròn hoặc Sys ML được trình bày trong Phụ lục C) để minh họa chức năng.*

Bảng A.1 *(kết thúc)*

Cơ sở hạ tầng: *Loại hỗ trợ cơ sở hạ tầng và/hoặc bảo vệ môi trường được cung cấp (ví dụ: đường dây điện, hệ thống quản lý cơ sở dữ liệu, bus dữ liệu có hoặc không có an toàn/bảo mật, bảo vệ IP, v.v...).*
An toàn: *Các yêu cầu liên quan đến an toàn đối với an toàn cấp độ mô đun và cấp hệ thống (ví dụ: để đáp ứng các mức tính năng bắt buộc) (Xem 5.1 – 5.3).*
Bảo mật: *Yêu cầu bảo mật cho bảo mật cấp mô đun và cấp hệ thống (ví dụ: chống truy cập trái phép hoặc đảm bảo mức độ riêng tư phù hợp, v.v.). Yêu cầu bảo mật này phải bao gồm các góc nhìn về phần cứng và phần mềm. (Xem 5.1, 5.4 – 5.7).*
Mô hình hóa: *Mô tả toán học hoặc vật lý của mô đun được áp dụng cho các tình huống thử nghiệm khác nhau (ví dụ: mô hình mô đun ảo).*

A.2 Phần mở rộng dành riêng cho phần cứng trong mẫu mô tả mô đun rô bốt

Đối với mẫu mô tả chung, xem Bảng A.1; bảng A.2 thể hiện các thông tin bổ sung nên cung cấp cho các mô đun có đặc điểm phần cứng.

Bảng A.2 – Các thông tin bổ sung đối với các mô đun có đặc điểm phần cứng

Thuộc tính của mô đun: *Danh sách các thuộc tính mô đun có đặc điểm phần cứng như kích thước vật lý, loại mặt lắp ghép, các đặc tính cơ học và điện.*
Đầu vào: *Danh sách các đầu vào như cảm biến kỹ thuật số/tương tự và các tín hiệu lệnh, cũng như các truyền thông khác giữa các mô đun, v.v…*
Đầu ra: *Danh sách các đầu ra, chẳng hạn như các đầu ra kỹ thuật số/tương tự, các đầu ra về góc/vị trí/tốc độ/mô men xoắn, v.v…*
Tính năng: *Với các mô đun có đặc tính phần cứng, điều này chủ yếu liên quan đến khả năng hoán đổi và khả năng tương tác. Mô đun được đề xuất phân chia theo quan điểm chức năng, chẳng hạn như các chi tiết/cấu trúc bên trong, khả năng kết nối với các mô đun bên ngoài và các tính năng liên quan trong môi trường hoạt động, bao gồm cả con người.*
Cơ sở hạ tầng: *Yêu cầu về cơ sở hạ tầng: Các yêu cầu của mô đun đối với phần còn lại của hệ thống, như nguồn điện khả dụng, hỗ trợ cấu trúc, tản nhiệt, v.v…* *Ràng buộc về môi trường: Các giới hạn của mô đun đối với các điều kiện bên ngoài như nhiệt độ, độ ẩm, sốc cơ học tối đa được phép, v.v..., cả khi tắt và khi đang hoạt động.*
Mô hình hóa: *Mô tả toán học hoặc vật lý của mô đun được áp dụng cho các mục đích khác nhau như mô phỏng hoạt động, đánh giá tính năng và các tình huống xác nhận.*

Phụ lục B

(tham khảo)

Ví dụ về mô đun rô bốt

B.1 Ví dụ về các mô đun có đặc tính phần cứng

B.1.1 Khớp quay chủ động

Tên mô đun: Khớp quay chủ động
Mô tả: Khớp của rô bốt hệ mô đun này nối hai khâu liền nhau và cung cấp chuyển động quay một bậc tự do. Khớp hệ mô đun này bao gồm động cơ, hộp giảm tốc, đường điện, đường tín hiệu và mạch điều khiển. Khớp có thể được dẫn động bằng điện. Khớp có thể cảm nhận góc quay và mô men xoắn của nó bằng các cảm biến bên trong.
Nhà sản xuất: ISO Inc.
Mã nhận dạng mô đun (ID): Joint J001
Ví dụ: Khớp có thể sử dụng để di chuyển cảm biến hoặc có thể kết hợp với các khớp khác (ví dụ 6 hoặc 7 bậc tự do) để tạo thành một tay máy.
Các đặc điểm phần cứng: - Kết nối kiểu mặt bích 001B ở cả 2 đầu với các đầu nối cho nguồn, CAN-bus, Safety-Torque-Off (chặn mô men xoắn an toàn – STO) - Cổng dịch vụ để truy cập trực tiếp vào thiết bị điện tử tích hợp qua USB - Cấp bảo vệ IP: IP 54
Các đặc điểm phần mềm: Giao thức truyền thông: CANOpen
Thuộc tính của mô đun: - Kích thước: ϕ80 mm x 70 mm - Khối lượng: 1,2 kg - Tỉ số giảm tốc: 1:30 - Phạm vi quay: ± 270 ^{o} - Tốc độ quay lớn nhất: 90 ^{o}/s - Mô men xoắn lớn nhất: 100 Nm / 20 Nm theo chiều quay về phía trước / về phía sau - Độ cứng vững của khớp: tối đa 0,5 mm/ 1° dịch chuyển ở tải trọng lớn nhất - Mô men danh định: 10 Nm - Dòng định mức của đầu nối: 10 A

- Công suất tiêu thụ: 50 W - Độ chính xác: ± 0,5 ° - Tính lặp lại: ± 0,3 ° - Giới hạn [mô men xoắn (Nm), vị trí (rad), tốc độ (rad/s)]
Đầu vào: - Vị trí (rad), tốc độ (rad/s), mô men xoắn (Nm) - Các tín hiệu cho các chức năng an toàn - Các thông số liên quan đến điều khiển
Đầu ra: - Giá trị thực tế của vị trí (rad), tốc độ (rad/s), mô men xoắn (Nm) - Trạng thái, các cảnh báo, lỗi, cường độ dòng điện, điện áp, nhiệt độ, thông tin chẩn đoán
Chức năng/Tính năng: Khớp có thể được sử dụng ở chế độ vị trí, chế độ vận tốc hoặc chế độ lực. Nó có thể được thiết lập để cung cấp cảnh báo chuyển sang chế độ dừng khi vượt quá giới hạn (không có chức năng an toàn). Có thể truy cập cấu hình bên trong (CAN ID, giới hạn, v.v...) qua USB.
Cơ sở hạ tầng: - Nguồn điện: 24 V DC (18 V ~ 30 V), 50 W - Điều kiện hoạt động: Nhiệt độ +5 đến +35 °C. Độ ẩm < 90 %, không ngưng tụ
An toàn: Tính năng an toàn được cung cấp phù hợp IEC 61800-5-2. Để bảo vệ mô đun (không có chức năng an toàn), mô đun dừng lại và chuyển sang trạng thái lỗi trong các trường hợp: lỗi do quá tải (cơ học, điện), cảm biến mã hóa bị lỗi, quá nhiệt. Nguồn điện cho rô bốt dịch vụ dùng trong hậu cần kho bãi cần được xác nhận để kiểm tra xem nó có tuân thủ các nguyên tắc cơ bản về khả năng tích hợp, khả năng hoán đổi và an toàn, v.v... hay không.
Bảo mật: Mặt bích 001B và nắp của cổng USB yêu cầu các dụng cụ tiêu chuẩn để tiếp cận
Mô hình hóa: Xem các tệp mô hình cho các mô hình động học và động lực học. Các tham số mô hình tĩnh bao gồm mô men giữ, mô men định mức và mô men dừng; các tham số mô hình động bao gồm tốc độ, gia tốc và băng thông.

B.1.2 Nguồn điện

Tên mô đun: Mô đun bộ nguồn kiểu pin
Mô tả: Mô đun pin với hệ thống quản lý nguồn, cung cấp đầu ra 24 V DC.
Nhà sản xuất: ISO Inc.
Mã nhận dạng mô đun (ID):

Bộ nguồn P001
Ví dụ: Bộ nguồn có thể sử dụng trong rô bốt di động hoặc trên bộ khung cơ học
Các đặc điểm phần cứng: Đầu nối nguồn (2 chân) Đầu nối dữ liệu vào/ra (4 chân) Cấp bảo vệ IP: IP 65
Các đặc điểm phần mềm: Giao thức truyền thông: RS232, Phần mềm quản lý pin kèm báo động
Thuộc tính của mô đun: - Thông số danh định: 24 V, 5 A liên tục, 20 A tối đa - Dung lượng: 5 Ah - Nguồn đầu ra: 25 V (đầy), 21 V (quản lý nguồn tắt) - Sạc: 28 V đến 33 V, dòng nạp đến 5A
Đầu vào: Đầu vào nguồn sạc Bật/tắt pin
Đầu ra: Đầu ra của nguồn Lỗi pin
Chức năng/Tính năng: Pin cần được bật qua đầu vào kỹ thuật số để cung cấp nguồn. Đầu ra kỹ thuật số phát tín hiệu cảnh báo sụt nguồn và lỗi
Cơ sở hạ tầng: Điều kiện hoạt động: Nhiệt độ +5 ° đến +35 °C. Độ ẩm < 90 %, không ngưng tụ
An toàn: Để bảo vệ mô đun (không có chức năng an toàn), mô đun dừng lại và chuyển sang trạng thái lỗi trong các trường hợp: quá tải, quá nhiệt, sụt nguồn, xả quá mức.
Bảo mật: Không áp dụng
Mô hình hóa: Vui lòng truy cập trang web (có cung cấp liên kết URL) để tải xuống mô hình hành vi cho các tình huống sử dụng. ,

B.2 Ví dụ về mô đun có đặc tính phần mềm

B.2.1 Nhận dạng

Tên mô đun: Mô đun nhận dạng thị giác
Mô tả:

Mô đun này có thể được sử dụng để nhận dạng khuôn mặt. Việc xây dựng cơ sở dữ liệu thường được tích hợp luôn bên trong một mô đun nhận dạng khuôn mặt nâng cao. Trong mô đun động, phần cứng, chẳng hạn như máy ảnh và máy quét ba chiều được sử dụng để cung cấp luồng dữ liệu tức thời. Kết quả của mô đun thay đổi, chẳng hạn như tỷ lệ khớp giữa dữ liệu mục tiêu đã cho và dữ liệu đã đăng ký trong cơ sở dữ liệu, số ID hoặc tên của mục khớp tốt nhất với dữ liệu trong cơ sở dữ liệu.

Nhà sản xuất:

ISO Inc.

Mã nhận dạng mô đun (ID):

VRM0001

Ví dụ:

Nhận dạng khuôn mặt

Các đặc điểm phần cứng:

Không

Các đặc điểm phần mềm:

Lấy dữ liệu (ảnh đầu vào), nhận dạng khuôn mặt, xuất kết quả (tên của khuôn mặt được nhận dạng)

Thuộc tính của mô đun:

- Nơi quản lý cơ sở dữ liệu, ví dụ: đường dẫn, IP và số hiệu cổng hoặc URL
- Các loại hạng mục nhận dạng được sử dụng, ví dụ như mắt, phần mặt phía trước, toàn thân, thân trên, v.v...
- Kích thước hình ảnh (pixel)
- Số khung hình mỗi giây (nếu đầu vào là một loại hình ảnh chuyển động)

Đầu vào:

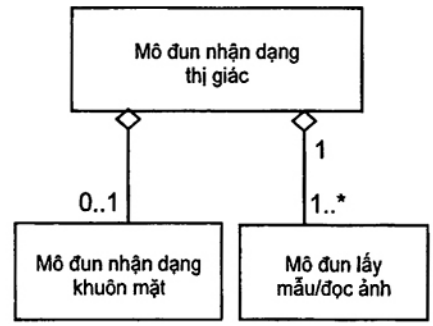
Hình ảnh hoặc luồng hình ảnh

Đầu ra:

Kết quả nhận dạng thị giác với độ tin cậy (hoặc độ chính xác) được chỉ định, ví dụ, tên của người được nhận dạng như James, Eve, Adam, v.v... (trong nhận dạng khuôn mặt)

Chức năng/Tính năng:

- Lấy dữ liệu hình ảnh (hoặc luồng hình ảnh) từ mô đun chụp ảnh để nhận dạng người
- Phát hiện khuôn mặt từ dữ liệu hình ảnh; Lấy ảnh khuôn mặt cùng với số nhận dạng của khuôn mặt đó; Trích xuất các điểm đặc trưng của khuôn mặt; Tính toán khoảng cách giữa chúng
- Tìm ảnh khuôn mặt (hoặc các điểm đặc trưng của khuôn mặt) từ cơ sở dữ liệu có sự trùng khớp gần nhất với giá trị đã tính toán này; Trả về số ID của ảnh khuôn mặt đã chọn



Cơ sở hạ tầng:

Phần mềm trung gian, cơ sở dữ liệu

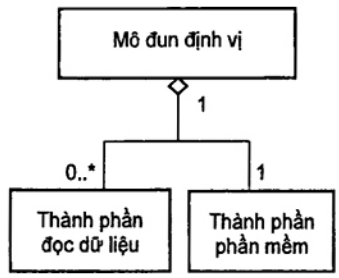
An toàn:

Không áp dụng cho các tình huống có các trường hợp sử dụng dự kiến

Bảo mật:

Xác thực, bảo mật cơ sở dữ liệu để đảm bảo quyền riêng tư
Mô hình hóa: Không áp dụng

B.2.2 Định vị

Tên mô đun: Mô đun định vị
Mô tả: Một rô bốt cá nhân cần phải biết tư thế của chính nó (vị trí và hướng) bên trong hệ tọa độ tham chiếu, quá trình nhận biết này được gọi là định vị. Mô đun định vị sử dụng một mô đun quét laser để xác định tư thế.
Nhà sản xuất: ISO Inc.
Mã nhận dạng mô đun (ID): ID do nhà sản xuất cung cấp
Ví dụ: Định vị dựa trên quét laser
Các đặc điểm phần cứng: Không
Các đặc điểm phần mềm: Lấy dữ liệu (ảnh đầu vào), tính toán và so sánh với các tham chiếu như các điểm mốc địa hình, đặt tư thế thành phần mềm lọc
Thuộc tính của mô đun: - Số lượng và loại các mô đun cảm nhận được sử dụng trong mô đun (ví dụ góc và số chùm tia của máy quét laser, v.v...) - Nơi quản lý thông tin về các điểm mốc địa hình, thông tin bản đồ hoặc thông tin về vùng nguy hiểm, ví dụ: đường dẫn, IP và số hiệu cổng hoặc URL
Đầu vào: Dữ liệu quét (từ mô đun quét laser) Dữ liệu về chuyển động từ mô đun điều khiển bánh xe, chẳng hạn như khoảng cách đi được và hướng.
Đầu ra: Tư thế của rô bốt cùng với mức tin cậy (hoặc độ chính xác)
Chức năng/Tính năng: - Lấy dữ liệu từ mô đun quét laser - Lấy dữ liệu từ mô đun điều khiển bánh xe - Lấy bộ ước lượng tư thế bằng cách sử dụng dữ liệu và bộ lọc - So sánh bộ ước lượng tư thế với các tư thế tham chiếu - Cập nhật tư thế 
Cơ sở hạ tầng:

Phần mềm trung gian
An toàn: Cảnh báo hoặc dừng theo tiêu chuẩn áp dụng nếu rô bốt đi vào vùng nguy hiểm
Bảo mật: Xác thực
Mô hình hóa: Không áp dụng

B.3 Ví dụ về các mô đun tổng hợp thường dùng

B.3.1 Quy định chung

Tất cả các rô bốt dịch vụ đều có những chức năng cao cấp có thể được xác định. Các chức năng này bao gồm giao diện người – rô bốt, điều hướng và định vị, thao tác, di chuyển từ nơi này đến nơi khác và đảm bảo an toàn theo các tiêu chuẩn an toàn hiện hành. Các mô đun rô bốt thường được sử dụng để tổ hợp các mô đun thực hiện các chức năng cấp cao điển hình như vậy. Điều này trình bày các mô đun ở cấp độ cao hơn chưa được thảo luận trước đây nhưng được coi là quan trọng để hiện thực hóa nhiều ứng dụng rô bốt dịch vụ.

Mô đun tổng hợp là sự kết hợp của các mô đun chứa các bộ phận cơ khí, điện tử và phần mềm. Các mô đun như vậy thường có bản chất phức tạp hơn, ví dụ như một tay máy hệ mô đun có nhiều bậc tự do với các bộ điều khiển tích hợp, cơ cấu dẫn động, cảm biến, phần mềm điều khiển, chức năng an toàn, v.v...

Đối với bất kỳ mô đun tổng hợp nào, các chức năng tối thiểu được trình bày trong mẫu mô tả phải được chỉ định trong hồ sơ thuộc tính và trong các định nghĩa đầu vào và đầu ra của mô đun. Đầu vào và đầu ra thường là dữ liệu được truyền đến/từ mô đun. Mẫu mô tả cho mọi mô đun thường dùng phải cung cấp tổng quan ngắn gọn và thông số kỹ thuật tối thiểu. Mỗi nhà sản xuất các mô đun như vậy có thể thêm nhiều chức năng hơn khi cần.

B.3.2 Mô đun tay máy

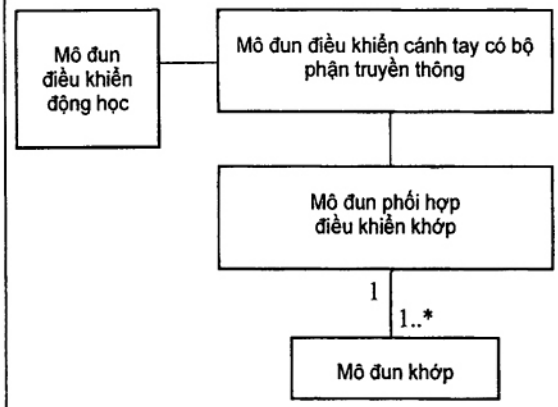
Điều khiển tay máy là một hoạt động phức tạp có thể liên quan đến nhiều cấp độ khác nhau của hệ mô đun như điều khiển khớp riêng lẻ, phối hợp thao tác di chuyển và sử dụng các khâu tác động cuối khác nhau.

Tên mô đun: Mô đun tay máy
Mô tả: Một tổ hợp lắp ráp từ các khâu cứng được kết nối thông qua các khớp tạo thành một hệ thống liên kết để điều khiển khâu tác động cuối với tất cả những bộ phận được kết nối tại các mặt lắp ghép cơ khí xác định. Nếu nhà sản xuất có ý định sử dụng mô đun trong ứng dụng cộng tác, thì thiết bị có thể cần thêm các chức năng liên quan đến an toàn, ví dụ như khi liên quan đến người cao tuổi hoặc trong môi trường chuyên nghiệp.

Nhà sản xuất: Thông tin liên hệ.
Mã nhận dạng mô đun (ID): Số tham chiếu sản phẩm duy nhất của nhà sản xuất cho cấu hình mô đun này
Ví dụ: Tay máy 6 bậc tự do có thể gắn khâu tác động cuối kiểu bàn tay 2 ngón. Thiết kế hệ mô đun cho phép người dùng cấu hình lại tay máy để có 4 đến 7 bậc tự do nhằm đáp ứng các yêu cầu cụ thể. Tay máy trong ví dụ này có cảm biến siêu âm có khả năng phát hiện vật thể ở khoảng cách 20 cm hoặc ngắn hơn.
Các đặc điểm phần cứng: Khung, vỏ, động cơ, mặt lắp ghép cơ khí
Các đặc điểm phần mềm: - Mô đun động học - Triển khai giao thức truyền thông - Mô đun điều khiển cánh tay - Mô đun phối hợp điều khiển khớp
Thuộc tính của mô đun: - Bậc tự do: loại khớp (2 chiều, 3 chiều, xoay/tịnh tiến), cấu hình tay máy - Phạm vi khớp: phạm vi dịch chuyển, dung sai dịch chuyển - Chiều dài và vị trí (hoặc loại) của mô đun liên kết các khớp - Tải trọng ở nhiều tư thế: Khối lượng cho phép (kg) hoặc lực (N) tại khâu tác động cuối trong trạng thái tĩnh và động - Phạm vi hoạt động của cánh tay (m x m x m) so với điểm tham chiếu của cánh tay - Tốc độ tối đa (m/s) và gia tốc (m/s^2) tại khâu tác động cuối (có thể phụ thuộc vào tư thế)
Đầu vào: Nhà sản xuất nên xác định một danh sách liệt kê các lệnh, ví dụ như: - Lệnh vị trí hoạt động cho tư thế, vận tốc - Di chuyển đến tư thế không gian được chỉ định trong quaternion (bộ bốn) - Giới hạn lực/tốc độ ở khâu tác động cuối
Đầu ra: Tư thế không gian thực tế được xác định theo x, y, z (mét) và hướng theo quaternion - Vận tốc không gian thực tế của khâu tác động cuối - Mặt bao không gian thực tế và hình chiếu của nó - Vận tốc khớp thực tế, gia tốc và lực (mô men xoắn) của từng cá thể (m/s, rad/s) - Trạng thái hoạt động, cảnh báo, lỗi, dòng thực tế, điện áp, nhiệt độ

Chức năng/Tính năng:

- Động học thuận, động học nghịch, lập kế hoạch chuyển động, động lực học
- Khởi động/dừng chuyển động (bật, tắt)
- Phát hiện quá tải, phát hiện trạng thái (tốt/lỗi), chức năng phanh/hãm, bật/tắt
- Cung cấp các giao diện dừng, tìm vị trí gốc
- Cung cấp các giao diện đặt/lấy lực/mômen xoắn, đặt/lấy vị trí, đặt/lấy vận tốc dựa trên giao diện trừu tượng
- Gửi giá trị lực/mô men xoắn cho tất cả các khớp theo định kỳ đến các khớp, nếu cần
- Dự báo chuyển động và mặt bao từ máy phát quỹ đạo để cải thiện hiệu suất



Cơ sở hạ tầng:

- Cấu trúc khâu/khớp để cung cấp hỗ trợ cơ học
- Khóa nhanh để gắn cơ cấu kẹp
- Nguồn điện
- Đường truyền dữ liệu
- Bộ điều khiển cục bộ và/hoặc phân tán của tay máy

An toàn:

Mô đun tuân theo các tiêu chuẩn an toàn hiện hành, như đã nêu tại Điều 5 (ví dụ IEC 61508-3 hoặc IEC 60204-1).

Chức năng dừng bảo vệ của mô đun tuân thủ mức tính năng (PL) "d" theo TCVN 7384-1 (ISO 13849-1).

An toàn cho mô đun: Mô đun cung cấp các chức năng an toàn sau:

- Giới hạn lực va chạm có mức tính năng "b" (da nhạy cảm)
- Giới hạn quá tải
- Kiểm soát giới hạn tốc độ theo ISO 10218 liên quan đến kiểm soát tốc độ

An toàn cho hệ thống: Mô đun cung cấp thông tin liên quan đến an toàn sau:

- Trạng thái mô đun
- Dự báo chuyển động và mặt bao từ máy phát quỹ đạo để giảm rủi ro va chạm (mức tính năng "a")
- Khoảng cách dừng được tính toán trong không gian ba chiều ở tốc độ định mức
- Tốc độ của khâu tác động cuối được thiết lập
- Chỉ định các lỗi bên trong có khả năng gây ra sự cố lớn hoặc suy giảm hiệu năng

Bảo mật:

- Mô đun có thể cung cấp một hoặc nhiều chức năng bảo mật sau:
- Tất cả các truyền thông mô đun – mô đun đều tuân theo các hướng dẫn trình bày tại Điều 7
- Tất cả các đầu vào sử dụng cơ chế phát hiện lỗi
- Chỉ chấp nhận đầu vào mục tiêu từ các nhà cung cấp được ủy quyền

- Thông tin lệnh chuyển động để sử dụng bao gồm cả ủy quyền
Mô hình hóa: Mô hình tĩnh và động ảo của tay máy bao gồm các khâu tác động cuối, động lực khớp và mặt bao

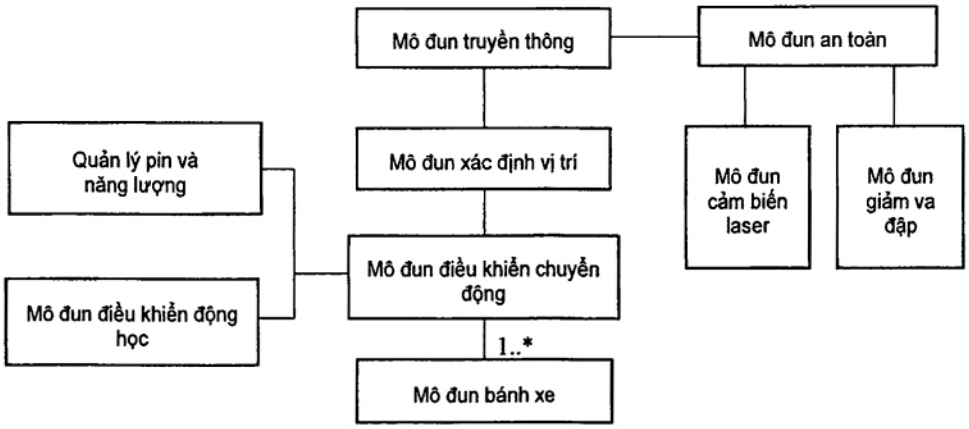
B.3.3 Mô đun sàn di động

Di động là một hoạt động phức tạp có thể liên quan đến nhiều cấp độ khác nhau của hệ mô đun như các cấu hình vận động, các hành vi di chuyển khác nhau và sự phối hợp thao tác khi di chuyển.

Tên mô đun: Mô đun sàn di động
Mô tả: Mô đun di động bao gồm: - Hệ thống chuyển động có thể bao gồm hệ thống treo, hệ thống lái, hệ thống dẫn động - Bộ phận mang tải trọng vận chuyển - Phương pháp di chuyển: bánh xe truyền thống, bánh xe đa năng (omniwheels), bánh xe bi, nhiều loại chân và cấu hình có chân, phương pháp di chuyển lai, leo trèo, bò, nhảy, v.v...
Nhà sản xuất: Thông tin liên hệ.
Mã nhận dạng mô đun (ID): Số tham chiếu sản phẩm duy nhất của nhà sản xuất cho cấu hình mô đun này
Ví dụ: Đế di động có bánh xe với các nút khẩn cấp, máy đo khoảng cách bằng laser và bộ giảm va đập (ba-đờ-xốc)
Các đặc điểm phần cứng: - Mô đun dẫn động - Mô đun giảm va đập - Mô đun pin - Phần cứng điều khiển đế di động - Mô đun máy đo khoảng cách bằng laser - Mô đun bộ phận cấu trúc - Các đặc điểm phần cứng của mô đun truyền thông
Các đặc điểm phần mềm: - Phần mềm điều khiển đế di động - Phần mềm cảm biến vị trí - Phần mềm truyền thông - Mô đun quản lý pin - Mô đun điều khiển hệ dẫn động động - Phần mềm cảm biến chạm - Mô đun phối hợp

- Trình quản lý an toàn
Thuộc tính của mô đun: - Cấu hình cơ học: Loại/số lượng bánh xe, cách sắp xếp và cấu hình bánh xe và kích thước tổng thể - Tải trọng vận chuyển: giới hạn tải trọng có thể mang trong các điều kiện môi trường được chỉ định (ví dụ: khối lượng, kích thước, nhiệt độ, v.v...) - Tốc độ di chuyển: tốc độ tối đa trong các tình huống vận hành dự kiến, đi thẳng, quay, đường phẳng/đường dốc, không tải, đầy tải - Trọng lượng, trọng tâm (COG) ở trạng thái không tải - Góc dốc tối đa và chiều cao bậc tối đa trong điều kiện không tải và đầy tải - Thời lượng pin và thời gian sạc lại để sử dụng đầy đủ
Đầu vào: Nhà sản xuất nên cung cấp một danh sách liệt kê các lệnh để sử dụng với mô đun rô bốt: - Tốc độ và hướng chuyển động - Các thông số liên quan đến điều khiển: điều kiện bề mặt, chướng ngại vật và môi trường - Phát hiện chướng ngại vật (kỹ thuật số và/hoặc tương tự) - Dừng bảo vệ và/hoặc dừng khẩn cấp
Đầu ra: - Tư thế không gian thực tế được xác định theo x, y, z (mét) và hướng theo quaternion - Thông tin quay của động cơ: hướng, góc - Gia tốc, mô men xoắn/dòng điện của động cơ - Trạng thái (tốt/lỗi), các cảnh báo, cường độ dòng điện, điện áp, nhiệt độ - Lỗi, các điều kiện vận hành liên quan đến an toàn - Mức tính năng an toàn (mức tính năng tùy thuộc vào ứng dụng có trường hợp sử dụng được đề xuất) - Phát hiện chướng ngại vật siêu âm tầm ngắn không an toàn - Trạng thái phát hiện chướng ngại vật - Trạng thái phát hiện bị kẹp - Trạng thái dừng bảo vệ và/hoặc dừng khẩn cấp
Chức năng/Tính năng: - Kiểm soát chuyển động cục bộ và động học - Bật/tắt chức năng - Phanh khẩn cấp - Kiểm tra trạng thái của các mô-đun bên trong

- Quản lý pin và năng lượng



Cơ sở hạ tầng:

- Khung gầm để cung cấp hỗ trợ cơ học
- Đường ray cung cấp điện
- Truyền thông

An toàn:

Mô đun tuân theo các tiêu chuẩn an toàn hiện hành, như đã nêu tại Điều 5 (ví dụ IEC 61508-3 hoặc IEC 60204-1).

- Khoảng cách dừng có thể lựa chọn ở các vận tốc cụ thể cho hệ thống được cấu hình
- Rô bốt cung cấp các mạch an toàn tích hợp để kết nối các cảm biến và mô đun liên quan đến an toàn.
- Các mức tính năng từ "a" đến "e" cho từng chức năng an toàn do mô đun cung cấp
- Mức tính năng do mô đun cung cấp: Dừng khẩn cấp (mức tính năng "d"), Đầu vào cho dừng bảo vệ (mức tính năng "d")

Bảo mật:

Mọi truyền thông giữa các mô đun phải tuân theo các hướng dẫn được trình bày trong Điều 5.

- Cơ chế phát hiện lỗi để đảm bảo tính toàn vẹn của dữ liệu truyền thông
- Các vị trí mục tiêu chỉ được chấp nhận từ các mô đun/nhà cung cấp được ủy quyền
- Lệnh chuyển động phải bao gồm thông tin ủy quyền để sử dụng

Mô hình hóa:

Mô hình tĩnh và động ảo của sàn di động

B.3.4 Mô đun tương tác người – rô bốt

Mô đun tương tác người – rô bốt (HRI) cung cấp phương tiện để con người tương tác với rô bốt, nhận biết ý định của rô bốt và cung cấp lệnh hoặc thông tin cho rô bốt.

Tên mô đun:

Mô đun tương tác người – rô bốt (HRI)

Mô tả:

Mô đun HRI có thể có các chức năng sau:

- Phát hiện/nhận dạng người - Tương tác với người (người dùng) qua lời nói, âm thanh, ánh sáng, màn hình cảm ứng
Nhà sản xuất: Thông tin liên hệ
Mã nhận dạng mô đun (ID): Số tham chiếu sản phẩm duy nhất của nhà sản xuất cho cấu hình mô đun này
Ví dụ: Chỉ có các thông báo và thông tin bằng giọng nói mới được gửi đến người dùng đã được camera nhận dạng và xác nhận đầu tiên. - Mô đun HRI có thể có các mô đun con bao gồm mô đun nhận dạng khuôn mặt, mô đun loa - Mô đun phần mềm phối hợp được sử dụng để quản lý trình tự giao diện hoặc dữ liệu của các mô đun con - Mô đun TTS (text to speech) dịch văn bản thành giọng nói - Đèn để chỉ trạng thái và chuyển động dự định
Các đặc điểm phần cứng: - Mô đun loa - Ánh sáng - Màn hình cảm ứng
Các đặc điểm phần mềm: - Mô đun phần mềm phối hợp - Phần mềm tương tác màn hình cảm ứng - Mô đun phần mềm TTS - Mô đun nhận dạng/xác nhận khuôn mặt
Thuộc tính của mô đun: - Mô đun phần mềm TTS, định dạng thông báo để phát ra loa - Mô đun nhận dạng khuôn mặt, định dạng cơ sở dữ liệu - API (giao diện lập trình ứng dụng) cho màn hình cảm ứng - Thông tin trạng thái và lỗi - Điều kiện hoạt động như nhiệt độ môi trường và phạm vi độ ẩm
Đầu vào: - Thông báo để phát ra loa - Dữ liệu đầu vào của người dùng từ màn hình cảm ứng
Đầu ra: - Kết quả phát hiện/nhận dạng người - Trạng thái (kết nối với cơ sở dữ liệu và máy chủ nhận dạng) - Lỗi (phát hiện hệ thống hoặc người) - Truyền dữ liệu đầu vào từ người dùng trên màn hình cảm ứng
Chức năng/Tính năng:

Mô đun nhận dạng khuôn mặt, thông qua mô đun nhận dạng:

- Chế độ hoạt động
- Mô đun phần mềm giọng nói, chuyển đổi văn bản thành giọng nói phát ra loa
- Mô đun phần mềm phối hợp, quản lý trình tự các giao diện và dữ liệu.
- Xử lý tương tác của người dùng thông qua màn hình cảm ứng
- Mô đun nhận dạng cử chỉ
- Mô đun nhận dạng lệnh thoại

Cơ sở hạ tầng:

Phần mềm trung gian, máy chủ nhận dạng ngoài, cơ sở dữ liệu ảnh và thông báo

An toàn:

Mô đun tuân theo các tiêu chuẩn an toàn hiện hành, như đã nêu tại Điều 5 (ví dụ IEC 61508-3 hoặc IEC 60204-1).

- Đánh giá quá trình phát triển mô đun cho an toàn chức năng (loạt tiêu chuẩn IEC 61508)
- Tin nhắn cảnh báo cho người dùng (theo các tiêu chuẩn ISO liên quan)
- Yếu tố con người và khả năng sử dụng

Bảo mật:

- Mô đun chỉ có thể truy cập thông qua dữ liệu được bảo mật
- Biện pháp ngăn chặn việc lạm dụng nhận dạng khuôn mặt bằng cách đảm bảo mức độ tin cậy tối thiểu
- Truy cập vào cơ sở dữ liệu và máy chủ nhận dạng thông qua kết nối an toàn

Mô hình hóa:

Không áp dụng

Phụ lục C

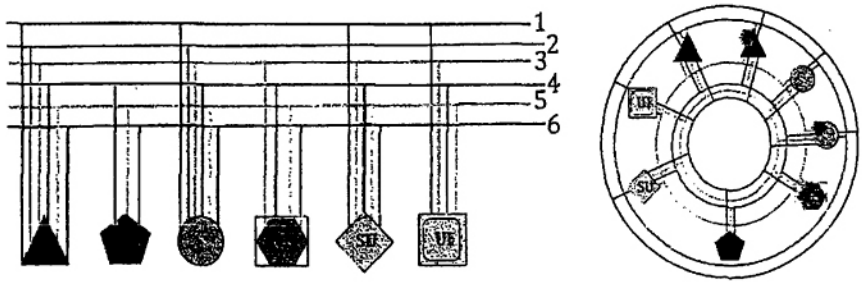
(Tham khảo)

Ví dụ về trường hợp sử dụng hệ mô đun cho rô bốt dịch vụ

C.1 Khái quát

Trong các phần sau sẽ trình bày các ví dụ điển hình về thiết kế hệ mô đun của rô bốt dịch vụ, áp dụng các khái niệm và hướng dẫn trong tiêu chuẩn này, bao gồm thiết kế phần cứng, thiết kế phần mềm cũng như các đặc điểm an toàn và bảo mật được trình bày trong các Điều 5 đến Điều 7. Trong Điều C.2, một hệ thống rô bốt di động cơ bản có thiết kế hệ mô đun đã được trình bày và các khái niệm về hệ mô đun được sử dụng để tích hợp các chức năng nâng cao, chẳng hạn như tay máy di động để cung cấp nhiều tính năng dịch vụ khác nhau. Ngoài ra, một rô bốt hỗ trợ cơ thể trong ứng dụng chăm sóc cá nhân được trình bày trong C.3.

Các vấn đề về kết nối khi cấu hình các mô đun có đặc điểm phần cứng có thể được trình bày dưới dạng sơ đồ. Hai phương pháp ví dụ, cụ thể là phương pháp đường thẳng và phương pháp vòng tròn dựa trên các công bố tương ứng của Virk [36] và Norman [37] được hiển thị trên Hình C.1 và có thể được sử dụng để minh họa khả năng kết nối giữa các mô đun trong thiết kế rô bốt dịch vụ. Tại đây, một tập hợp các biểu tượng mô đun thông dụng được xác định và kết nối để tạo thành các thiết kế ứng dụng cụ thể.



CHÚ DẪN:

1	môi trường	3	dữ liệu	5	an ninh
2	cơ học	4	nguồn	6	an toàn

	cảm biến		phần mềm mô đun máy tính		cảm biến xử lý
	nguồn điện		phần mềm		người giám sát
	bộ truyền động		bộ truyền động với xử lý		giao diện người dùng

Hình C.1 – Sơ đồ kết nối cho hệ mô đun của rô bốt và các mô đun mẫu

Phương pháp đường thẳng trình bày các biểu tượng mô đun được xác định có khả năng kết nối với các mô đun khác được minh họa như sơ đồ đường truyền dữ liệu thông thường thông qua các biến tương tác được chỉ định. Các tương tác này bao gồm an toàn, bảo mật, nguồn điện, truyền thông dữ liệu (được biểu diễn theo nhiều cách khác nhau như một đường truyền dữ liệu kỹ thuật số cụ thể, hoặc như các đường tín hiệu tương tự hoặc kỹ thuật số đơn giản), các mặt lắp ghép cơ khí và các biện pháp bảo vệ thích hợp cho môi trường hoạt động (ví dụ: nước, bụi, rung động, v.v...). Phương pháp vòng tròn cũng trình bày chi tiết kết nối hệ mô đun thông qua định dạng hình tròn. Cả hai phương pháp đều có thể hoán đổi cho nhau và cho phép thiết kế và trình bày các chức năng cụ thể bằng cách kết nối các khối riêng lẻ thông qua giao diện cho các yêu cầu tương tác liên quan.

Nhiều mô đun có thể bao gồm các tính năng thông minh, trong trường hợp đó chúng sẽ yêu cầu một loạt các chức năng kết nối dữ liệu cho các yêu cầu tương tác. Ví dụ, mô đun nguồn điện có thể có các tính năng quản lý nguồn điện thông minh và do đó có thể cần kết nối dữ liệu; điều này có thể đạt được thông qua một loạt các giao thức (ví dụ: CAN, I2C, TCP/IP, USB).

Có những phương pháp và cách tiếp cận khác để thể hiện các đặc điểm hệ mô đun bên trong một hệ thống tùy thuộc vào ứng dụng (ví dụ: SysML).

C.2 Hệ mô đun cho hệ thống rô bốt di động

Một ví dụ về rô bốt dịch vụ có thiết kế hệ mô đun là rô bốt giao hàng dựa trên sàn di động có thể hoạt động trong môi trường đông đúc để giao đồ vật cho con người, bao gồm một sàn di động và nhiều cảm biến khác nhau được sử dụng để nhận dạng đồ vật. Các hành vi chính của nó khi sử dụng phương pháp tiếp cận của Brook [38] như sau:

- Di chuyển đến một vị trí mong muốn cụ thể
- Xác định đồ vật và tránh các mối nguy hiểm tiềm ẩn trong quá trình di chuyển

Hình C.2 a) cho thấy cấu hình các mô đun có đặc tính phần cứng và phần mềm cho một rô bốt dịch vụ giao hàng có thể điều hướng với hành vi tránh chướng ngại vật trong các cơ sở đông đúc trong khi vẫn đảm bảo an toàn cho dữ liệu không bị những người không được phép truy cập thông qua mã hóa. Hình C.2 b) cho thấy một ví dụ trực quan. Tình huống cho trường hợp sử dụng này là phải lường trước các chú ý về an toàn, về bảo mật và về bảo mật liên quan đến an toàn. Để đáp ứng yêu cầu về an toàn, các mô đun được sử dụng phải cho phép đáp ứng các yêu cầu an toàn cần thiết cho rô bốt dịch vụ giao hàng trong lĩnh vực ứng dụng. Rô bốt dịch vụ giao hàng có nhiều loại mô đun có đặc điểm phần cứng khác nhau, bao gồm các mô đun bánh xe, mô đun dẫn động, mô đun LIDAR, mô đun camera hình ảnh hai chiều, mô đun camera hồng ngoại, mô đun tính toán và mô đun cấp nguồn. Bốn bánh xe chủ động được lắp trên một sàn di động và được điều khiển bởi mô đun tính toán để thực hiện các chuyển động di chuyển mong muốn. Lưu ý rằng các mô đun phải tuân theo các quy trình được đề xuất tại Điều 5, trong đó việc đánh giá rủi ro an toàn, bảo mật và an toàn liên quan đến bảo mật phải thực hiện tương ứng với ứng dụng cụ thể của rô bốt giao hàng. Thông tin (hoặc thuộc tính) liên quan đến đặc điểm phần cứng

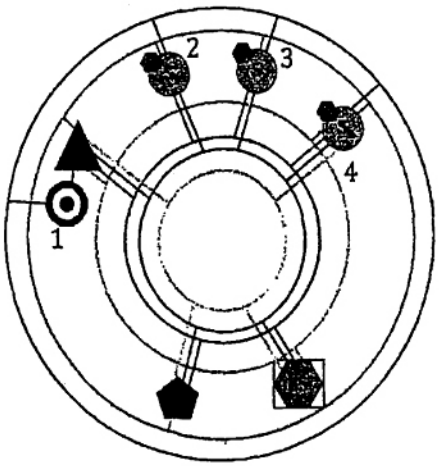
phải được cung cấp để đảm bảo hoạt động đúng của các mô đun phần mềm tương ứng. Đặc biệt, các mô đun cơ học để giao hàng phải được tổ chức tốt để có thể dễ dàng cấu hình lại. Các đối tượng tĩnh có trong môi trường hoạt động phải được xác định để thực hiện các hành vi phù hợp như hướng về phía mục tiêu hoặc tránh chướng ngại vật. Các đối tượng liên quan đến an toàn động (như con người) phải có các yêu cầu an toàn nghiêm ngặt hơn.

Hình C.2 c) minh họa cấu hình các mô đun phần mềm có thể đạt được các hành vi mong muốn bằng cách sử dụng các mô đun có đặc tính phần cứng, được hiển thị trên hình C.2 a). Để thuận tiện, việc ánh xạ giữa các đặc điểm phần cứng và phần mềm của các mô đun không được xem xét ở đây. Thay vào đó, chức năng tổng thể của các mô đun phần mềm khác nhau cần thiết trong tình huống cho trường hợp sử dụng được nêu bật trên Hình C.2 c). Các mô đun phần mềm cho một rô bốt dịch vụ giao hàng có thể được sắp xếp như sau:

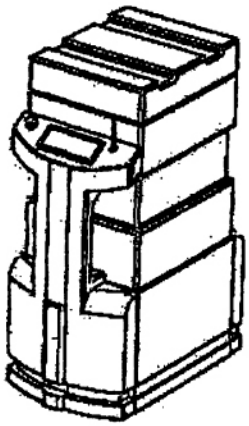
1) một mô đun nhận dạng,
2) một hoặc nhiều mô đun trao đổi dữ liệu,
3) một mô đun bảo mật,
4) một mô đun dẫn đường,
5) một mô đun tránh chướng ngại vật,
6) một mô đun điều khiển di chuyển và
7) một mô đun an toàn.

Mô đun nhận dạng có thể bao gồm mô đun nhận dạng cá nhân để nhận dạng khuôn mặt của những cá nhân được ủy quyền và mô đun nhận dạng đối tượng để nhận dạng các đối tượng liên quan đến an toàn. Mô đun trao đổi dữ liệu được sử dụng để trao đổi dữ liệu giữa các mô đun trong rô bốt giao hàng, máy chủ và các rô bốt khác khi thích hợp. Các lệnh như di chuyển đến vị trí mục tiêu và nhận dạng một người cụ thể được nhận qua mô đun trao đổi dữ liệu. Do đó, các lệnh phải được mã hóa/bảo vệ và cần xác thực quyền để được phân phối và đọc bởi các mô đun có đúng thẩm quyền. Nếu giải mã không thành công hoặc thẩm quyền đối với lệnh đã cho không đúng, mô đun bảo mật phải phát cảnh báo, theo dõi tiến trình của các hoạt động và thực hiện các biện pháp bảo mật phù hợp. Nếu tình huống bảo mật xảy ra có thể dẫn đến các vấn đề về an toàn, mô đun phải thông báo cho mô đun an toàn để đảm bảo các biện pháp an toàn phù hợp có thể được triển khai. Mô đun điều hướng bao gồm mô đun lập bản đồ, mô đun định vị và mô đun lập kế hoạch đường đi. Mô đun điều hướng gửi điểm lộ trình tiếp theo cho mô đun điều khiển di chuyển. Ngoài ra, mô đun điều hướng còn kiểm tra liệu rô bốt có đang hoạt động trong khu vực nguy hiểm hay không và sau đó sẽ gửi thông báo báo động đến mô đun an toàn nếu rô bốt rơi vào tình huống nguy hiểm. Mô đun tránh chướng ngại vật sẽ cung cấp cho mô đun điều hướng thông tin về chướng ngại vật để rô bốt tránh. Tất nhiên, mô đun tránh chướng ngại vật có thể được tích hợp vào mô đun điều hướng. Mô đun an toàn sẽ quản lý các mối nguy hiểm liên quan đến an toàn cho rô bốt, bao gồm cả những mối nguy hiểm liên quan đến an ninh được xác định khi xem xét các

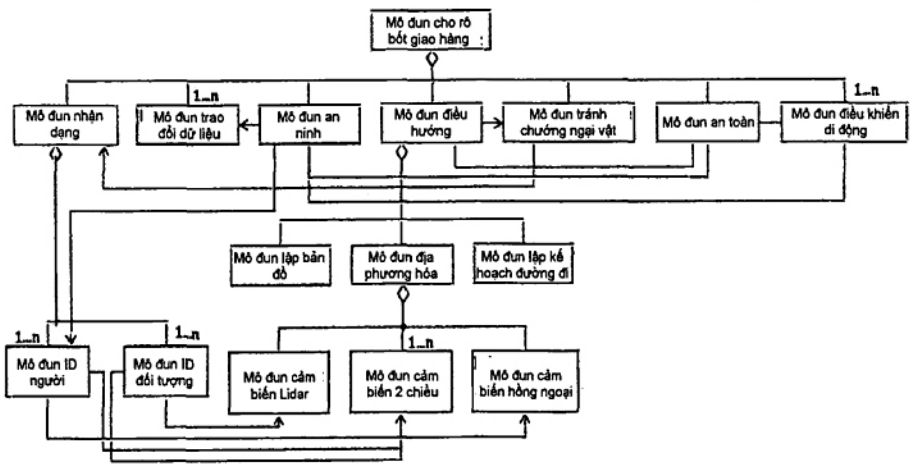
rủi ro an toàn và an ninh. Mô đun an toàn sẽ thu thập và phân tích dữ liệu liên quan đến an toàn từ mô đun nhận dạng, mô đun trao đổi dữ liệu, mô đun an ninh, mô đun điều hướng và mô đun điều khiển di chuyển. Mô đun điều khiển di chuyển bao gồm mô đun phần mềm để điều khiển bốn cơ cấu dẫn động (A_{1-4}) trong các mô đun bánh xe. Dựa theo kết quả phân tích, các biện pháp an ninh, an toàn và an toàn liên quan đến an ninh phù hợp sẽ được xem xét và thực hiện. Mô đun định vị tạo ra tư thế hiện tại của rô bốt thông qua các mô đun cảm biến (ở đây gồm mô đun cảm biến LIDAR, mô đun cảm biến camera hai chiều và mô đun cảm biến camera hồng ngoại) để thu thập thông tin cảm biến cần thiết bằng các mô đun phần mềm phù hợp. Lưu ý rằng các tệp thuộc tính của các mô đun phần mềm được sử dụng cho rô bốt dịch vụ giao hàng phải được cung cấp để đảm bảo hoạt động theo kế hoạch. Phần tô bóng trong các ô hiển thị trên Hình C.2 c) biểu thị các mô đun phần mềm đang truyền tin với các mô đun có đặc điểm phần cứng.



a) Mô đun với phần cứng



b) Ví dụ về hình ảnh rô bốt giao hàng



c) Các mô đun phần mềm

CHÚ DẪN:

1 bánh xe 2 camera hồng ngoại 3 cảm biến LIDAR 4 camera 2 chiều

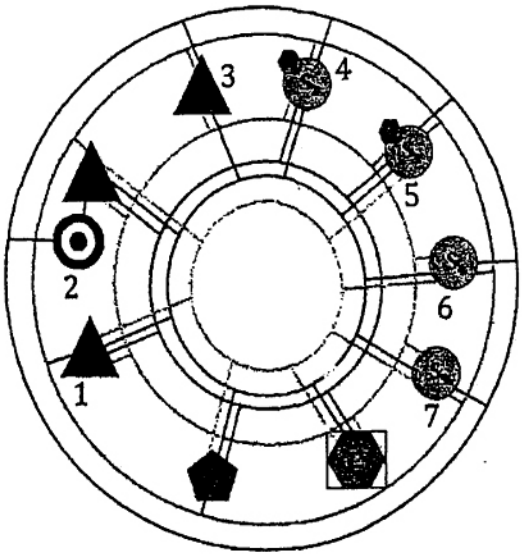
Hình C.2 – Ví dụ về thiết kế rô bốt giao hàng kiểu sàn di động

Để mở rộng tính năng của rô bốt giao hàng kiểu sàn di động nhằm thực hiện các hành vi của tay máy di động, có thể tích hợp thêm các thao tác nhặt và cùng các thao tác di chuyển để rô bốt nâng cao có thể lấy đồ vật từ một nơi, di chuyển đến một địa điểm khác và giao đồ vật cho con người. Các hành vi thao tác có thể như sau:

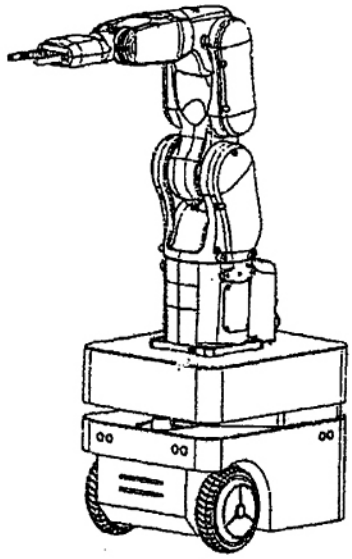
- Lấy và đặt đồ vật
- Lấy đồ vật – di chuyển – đặt đồ vật
- Xác định các vật thể và tránh các rủi ro tiềm ẩn trong quá trình thao tác

Sau khi điều hướng đến vị trí đã chỉ định, rô bốt có thể được vận hành để định vị chính xác tay máy của nó về phía đối tượng mục tiêu để hoàn thành tác vụ lấy đồ vật yêu cầu. Thông thường, việc định vị chính xác nên được kết hợp với việc tinh chỉnh thông qua sự trợ giúp của dữ liệu phản hồi từ cảm biến phù hợp, chẳng hạn như từ hệ thống thị giác. Trên hình C.3, sáu mô đun dẫn động ($A_{3\text{-}8}$] hợp tác với các mô đun cảm biến được thiết kế để hoàn thành tác vụ lấy đồ vật. Ưu điểm của việc áp dụng phương pháp tiếp cận hệ mô đun là các mô đun liên quan đến tay máy có thể dễ dàng được đưa lên sàn di động hiện có để đồng thời chia sẻ các liên kết dữ liệu chung về thông tin cảm biến theo cách an toàn với các mô đun khác, cũng như sử dụng cùng một mô đun cấp điện (P), cùng một mô đun tính toán có phần mềm (CS) và cùng các mô đun cảm biến (S_1-S_3] như những mô đun trên sàn di động. Do đó, ưu điểm của việc áp dụng phương pháp tiếp cận hệ mô đun trong ví dụ về rô bốt kiểu sàn di động này là mỗi hành vi và chức năng có thể đạt được bằng cách sử dụng sự kết hợp phù hợp giữa các mô đun và các kết nối giao diện được thiết kế, tạo ra một cách thuận tiện để ghép nối thêm các mô đun khác nhằm cải tiến toàn diện thiết kế cho các ứng dụng khác.

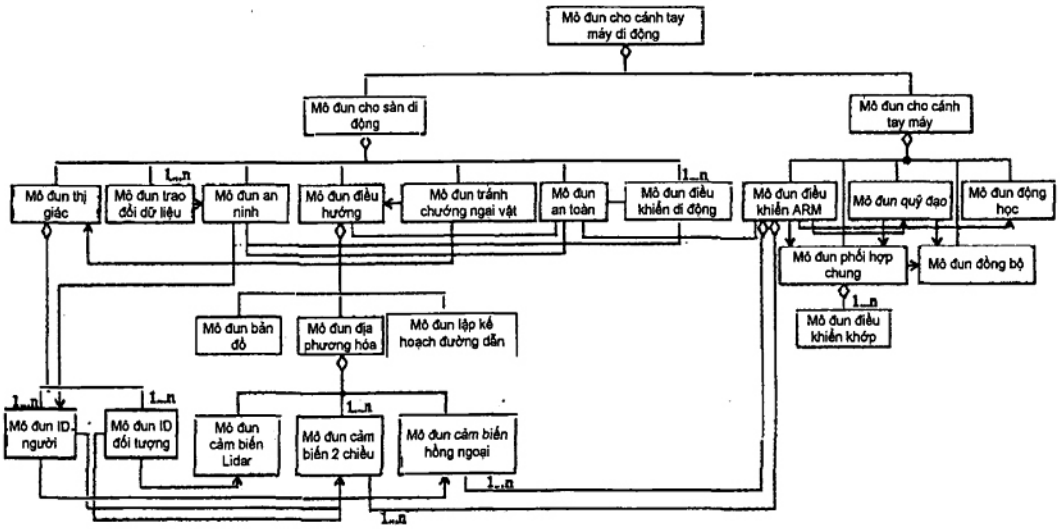
Đối với tay máy di động, một số mô đun phần mềm để điều khiển các đối tượng mục tiêu được thêm vào các mô đun phần mềm cho rô bốt dịch vụ giao hàng. Đặc biệt, các vấn đề an toàn, an ninh và an toàn liên quan đến an ninh phải được đảm bảo để điều khiển tay máy, sàn di động và mô đun điều khiển phải kiểm tra và sử dụng dữ liệu từ các mô đun cảm biến camera hai chiều/hồng ngoại dưới sự quản lý chặt chẽ của mô đun an toàn. Tất nhiên, mô đun điều khiển cánh tay phải nhận tư thế của đối tượng mục tiêu từ mô đun cảm biến camera và tạo ra quỹ đạo cần thiết để đạt được tư thế đã cho bằng cách sử dụng mô đun động học. Mô đun phối hợp khớp phải nhận quỹ đạo đã tạo và gửi khoảng cách và hướng cần di chuyển đến các mô đun điều khiển khớp để điều khiển từng cơ cấu dẫn động một cách phù hợp. Đặc biệt, mô đun đồng bộ phải sử dụng thông tin đồng bộ hóa các khớp trong mô đun phối hợp khớp.



a) Mô đun với phần cứng



b) Ví dụ về hình ảnh của cánh tay máy di động



a) Mô đun với phần mềm

CHÚ DẪN:

1	bộ truyền động tay máy	5	camera 2 chiều
2	bánh xe	6	màn hình cảm ứng
3	loa	7	Micro
4	cảm biến LIDAR		

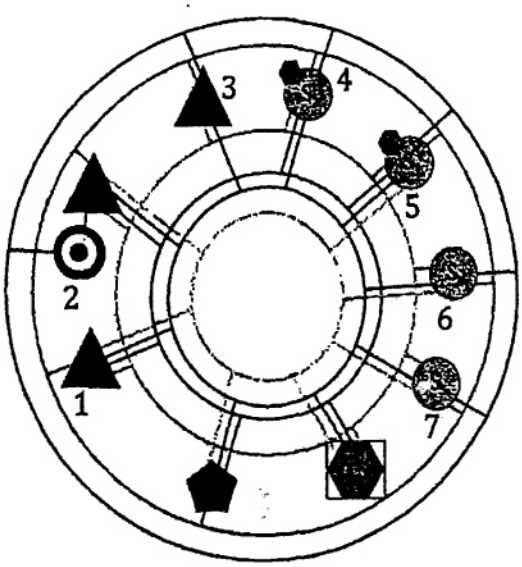
CHÚ THÍCH 1: Mô đun bảo mật và Mô đun an toàn có thể được đặt trong Mô đun điều khiển

CHÚ THÍCH 2: Khuyến nghị rằng các mô-đun SW cho sàn di động và bộ điều khiển hoạt động trên các bo mạch máy tính độc lập.

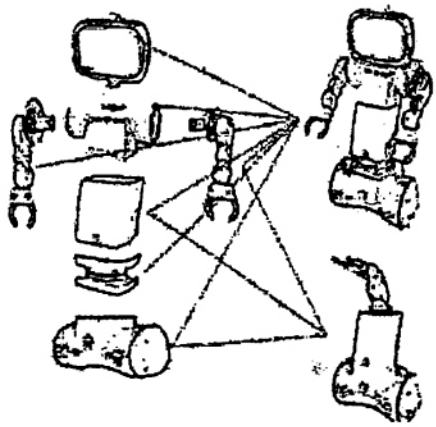
Hình C.3 – Ví dụ về thiết kế tay máy di động

Rô bốt phục vụ di động được thiết kế để di chuyển trong môi trường gia đình hoặc công cộng để thực hiện nhiều tác vụ phục vụ hoặc tương tác với con người. Một giao diện tự nhiên để tương tác với con người cần được sử dụng để cho phép người thường sử dụng rô bốt theo cách tự nhiên trong khi họ tránh va chạm với các chướng ngại vật liên quan đến an toàn, cố định và di động. Để thực hiện các hành vi được chỉ định từ con người, rô bốt phục vụ phải có khả năng nhận hướng dẫn hoặc thông tin của con người thông qua một số giao diện người dùng, chẳng hạn như giao diện đồ họa, giao diện đàm thoại và giao diện cử chỉ. Do đó, để mở rộng rô bốt giao hàng kiểu sàn di động và mô đun tay máy, hành vi chính phải đưa vào một mô đun tương tác người – rô bốt. Các hành vi cho các mô đun người – rô bốt gồm:

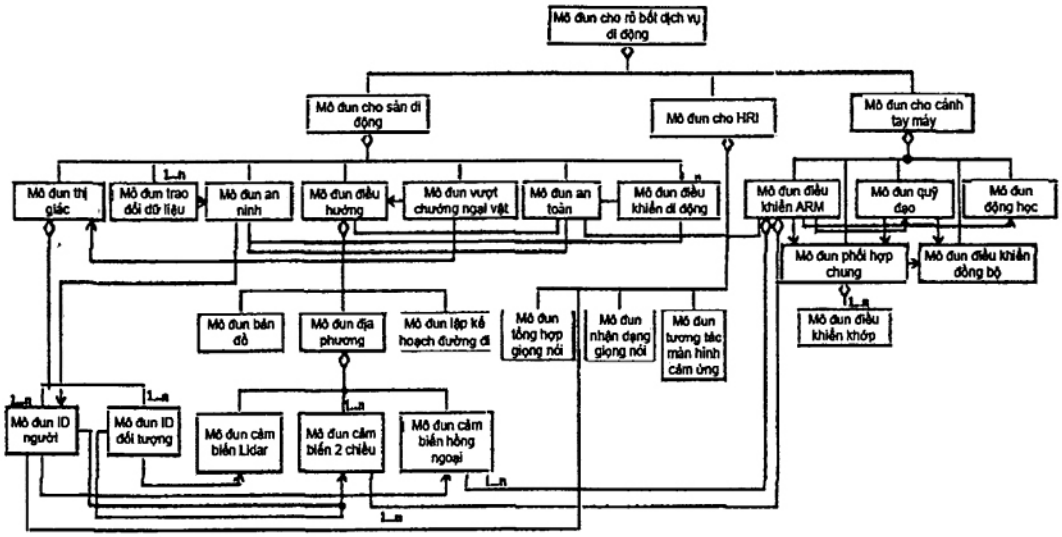
- Tương tác bằng giọng nói
- Tương tác bằng cử chỉ
- Tương tác bằng màn hình cảm ứng



a) Mô đun với phần cứng



b) Rô bốt dịch vụ di động



c) Mô đun phần mềm

CHÚ DẪN:

1	bộ truyền động tay máy	5	camera 2 chiều
2	bánh xe	6	màn hình cảm ứng
3	loa	7	Micro
4	cảm biến LIDAR		

CHÚ THÍCH 1: Mô đun bảo mật và Mô đun an toàn có thể được đặt trong Mô đun cánh tay máy.

CHÚ THÍCH 2: Khuyến nghị rằng các mô-đun SW cho sàn di động và bộ điều khiển hoạt động trên các bo mạch máy tính độc lập.

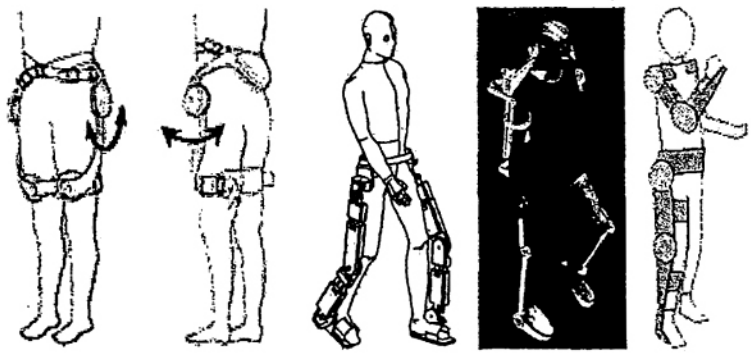
Hình C.4 – Thiết kế cho rô bốt phục vụ di động

Trên Hình C.4 có hai cảm biến được đưa vào để nhận hướng dẫn của con người. Đầu tiên là mô đun màn hình cảm ứng (S_4) để cung cấp giao diện đồ họa, do đó người dùng có thể ra lệnh cho rô bốt một

cách trực tiếp và rõ ràng. Thứ hai là mô đun cảm biến micrô (S_5) để cho phép giao diện đàm thoại, do đó người dùng có thể ra lệnh bằng giọng nói theo cách nói tự nhiên. Tất cả các cảm biến một lần nữa có thể chia sẻ cùng một nguồn cấp điện (P), các mô đun tính toán (CS) và các mô đun cảm biến gốc (S_2-S_3) như những cảm biến trong tay máy di động trên Hình C.3. Đối với rô bốt phục vụ di động, một số mô đun phần mềm cho HRI được thêm vào các mô đun phần mềm cho tay máy di động. Các mô-đun phần mềm bổ sung cho HRI nên bao gồm mô đun nhận dạng giọng nói cho các ngôn ngữ khác nhau, mô đun tổng hợp giọng nói, mô đun tương tác màn hình cảm ứng để điều khiển màn hình cảm ứng và mô đun cảm biến camera hai chiều/hồng ngoại để phát hiện tư thế của các vật thể và người. Đặc biệt, cần lưu ý rằng mô đun tương tác màn hình cảm ứng được liên kết với mô đun bảo mật để quản lý việc kiểm soát truy cập nhằm ngăn chặn những người không được phép truy cập vào rô bốt.

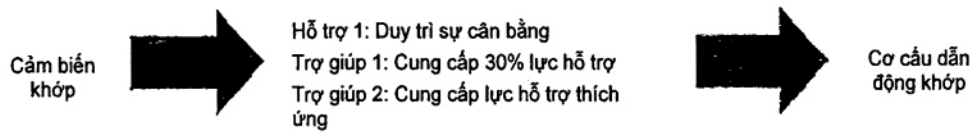
C.3 Hệ mô đun cho hệ thống rô bốt kiểu bộ khung cơ học

Rô bốt hỗ trợ cơ thể được thiết kế để giúp người dùng thực hiện các tác vụ chuyển động cần thiết bằng cách cung cấp bổ sung hoặc tăng cường khả năng cá nhân. Theo quan điểm hệ mô đun, điều này có thể tập trung vào việc sử dụng các mô đun có thể hoán đổi cho nhau để phù hợp với giao diện nhiều khớp của con người và các hình thức áp dụng năng lượng bên ngoài nhằm hỗ trợ chuyển động cần thiết của con người. Mục này chỉ tập trung vào các rô bốt hỗ trợ cơ thể kiểu bộ khung cơ học có thể đeo được và một số ví dụ được trình bày trên Hình C.5.



Hình C.5 – Rô bốt hỗ trợ cơ thể cho các ứng dụng chăm sóc cá nhân
(từ trái qua: các bộ khung cơ học cho hông, thân dưới, thân dưới và vai, và toàn thân)

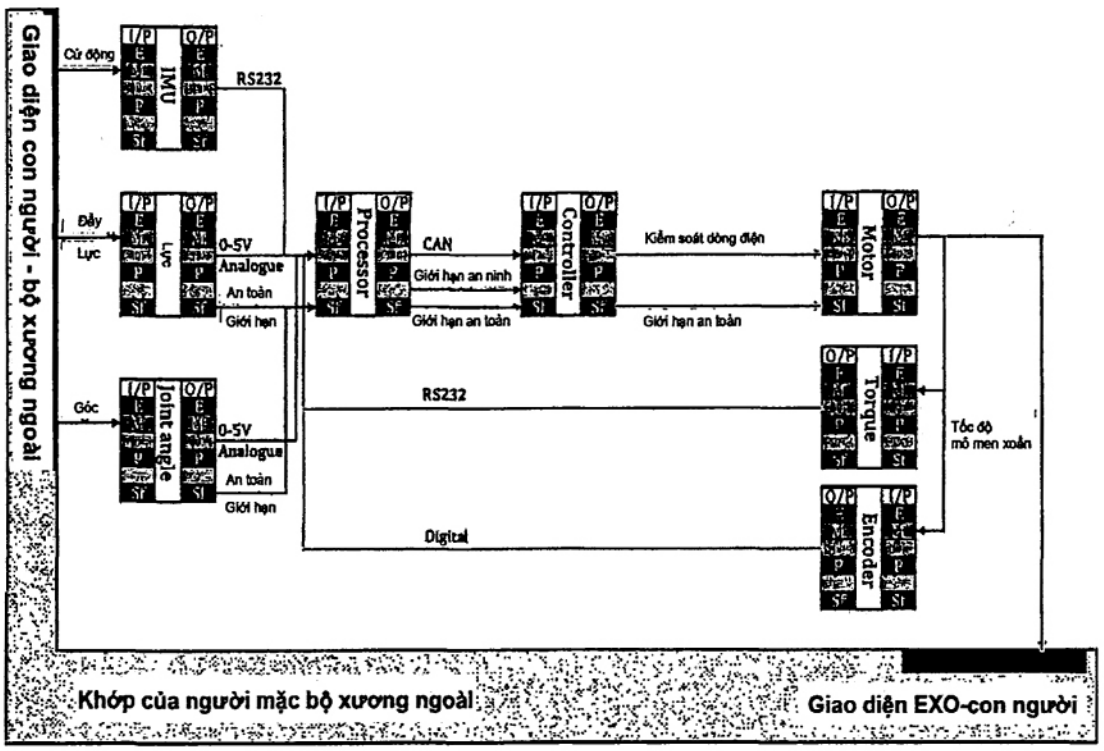
Bộ khung cơ học di động kiểu đeo có thể được sử dụng để hỗ trợ nhiều tác vụ chuyển động của con người như giữ ổn định khi đứng, hỗ trợ cơ thể cho việc chuyển từ ngồi sang đứng/đứng sang ngồi, đi bộ



và leo lên/xuống cầu thang. Bộ khung cơ học kiểu đeo này cũng có thể được sử dụng cho các ứng dụng tập luyện, các chế độ hoạt động khác nhau có thể được mô tả trong một tập hợp các hành vi như được trình bày trên Hình C.6.

Hình C.6 – Hành vi hoạt động của bộ khung cơ học di động kiểu đeo

Các hành vi có thể đạt được bằng cách áp dụng phương pháp tiếp cận hệ mô đun để kiểm soát chuyển động mong muốn tại một khớp riêng lẻ của người. Hình C.7 cho thấy các đặc điểm chung trong việc tuân theo phương pháp thiết kế này để áp dụng lực phục hồi/hỗ trợ cơ thể cho một khớp đơn bằng cách sử dụng các mô đun cảm biến chuyển động của con người, bao gồm các cảm biến như thiết bị đo quán tính (IMU), cảm biến lực và góc khớp để phát hiện ý định chuyển động của khớp mong muốn làm đầu vào để xác định thông tin nhằm điều khiển động cơ để cung cấp mô men xoắn cần thiết cho khớp. Các vấn đề an toàn trong Điều 5 nên được đưa vào để đáp ứng các giới hạn liên quan đến góc khớp an toàn thông qua các giao thức ghép nối của các mô đun rô bốt được áp dụng trong thiết kế. Lưu ý một số vấn đề được lược bỏ cho dễ đọc như chi tiết về nguồn điện, bảo mật dữ liệu chuyển động của con người và các khía cạnh về môi trường.



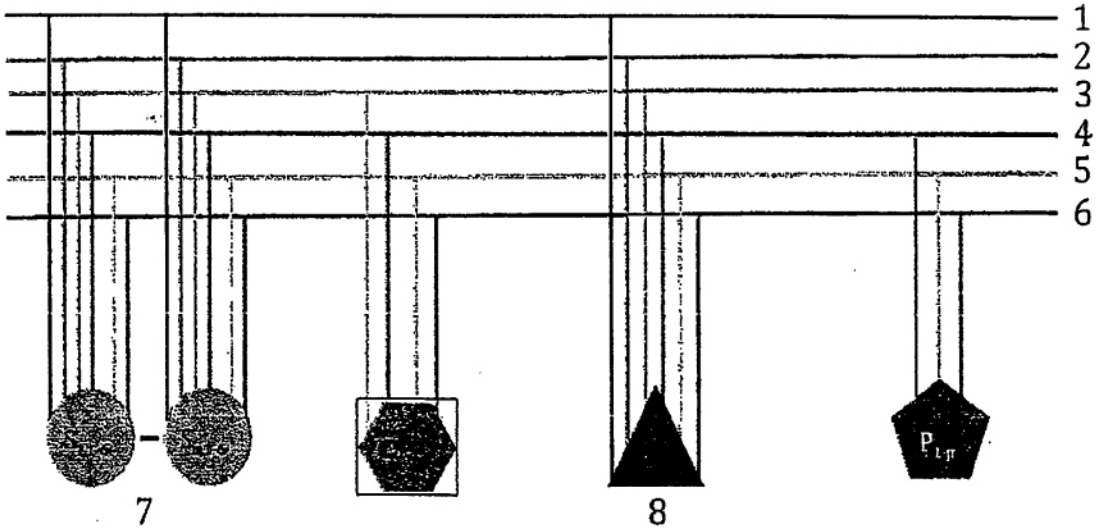
CHÚ DẪN:

I/P	đầu vào	O/P	đầu ra
E	môi trường	P	nguồn
M	cơ học	Sc	an ninh
D	dữ liệu	Sf	an toàn

Hình C.7 – Thiết kế khung cơ học hỗ trợ có điều khiển cho khớp đơn

Một khung chuẩn hệ môđun như vậy cho các khớp ở phần dưới cơ thể có thể được thiết kế và các hệ thống con ở cấp độ khớp này có thể được kết nối trong các kiến trúc được cấu hình phù hợp để hiện thực hóa bộ khung cơ học kiểu đeo như mong muốn. Bằng cách này, các khớp của con người sẽ được điều khiển để có được hệ thống hỗ trợ chuyển động mong muốn. Ví dụ, Hình C.8 cho thấy cách các

khớp hông, đầu gối và mắt cá chân của cả hai chân nên được kết nối thông qua sáu bộ cảm biến và cơ cấu dẫn động để xác định bộ khung cơ học sáu bậc tự do kiểu đeo để hỗ trợ các chuyển động của con người như đi bộ trong mặt phẳng dọc, được thể hiện bằng phương pháp đường thẳng, trong đó *n* là số lượng cảm biến được sử dụng tại các khớp hông, đầu gối và mắt cá chân, *m* là số lượng mô đun tính toán có phần mềm được sử dụng và *p* là số lượng nguồn điện được sử dụng cho cả bộ khung cơ học.



CHÚ DẪN:

1	môi trường	5	an ninh
2	cơ học	6	an toàn
3	dữ liệu	7	cảm biến cho khớp hông, đầu gối và mắt cá chân
4	nguồn	8	Bộ truyền động cho khớp hông, đầu gối và mắt cá chân

Hình C.8 – Khung cơ học 6 bậc tự do để hỗ trợ các tác vụ chuyển động, ví dụ như đi bộ

Phụ lục D

(Tham khảo)

Hướng dẫn về thử nghiệm mô đun rô bốt

D.1 Giới thiệu chung

Các nhà sản xuất mô đun rô bốt phải thử tính năng, an toàn và bảo mật của các mô đun và khi thích hợp, phải cung cấp bằng chứng đầy đủ thu được qua các phương pháp thử nghiệm được thiết kế phù hợp để xác nhận rằng các mô đun của họ phù hợp với các trường hợp sử dụng dự kiến.

CHÚ THÍCH: Mục đích lâu dài là xây dựng các phương pháp thử được chấp nhận rộng rãi cho các nhà sản xuất mô đun trong các bản sửa đổi tương lai của tiêu chuẩn này.

Phiên bản hiện tại hỗ trợ xây dựng các phương pháp thử bằng cách đề xuất các phương pháp thử tham khảo để các nhà sản xuất khám phá nhằm thử nghiệm các nguyên tắc hệ mô đun của các sản phẩm mô đun rô bốt của họ. Các nhà sản xuất nên thực hiện quy trình xác nhận và kiểm định trên các mô đun của họ.

D.2 Xác định các thử nghiệm cần thiết

Các nhà sản xuất mô đun rô bốt nên xây dựng các phương pháp thử để thiết lập các đặc điểm về an toàn, bảo mật và hiệu suất phù hợp với các nguyên tắc hệ mô đun được trình bày trong Điều 4 và các hướng dẫn được trình bày trong Điều 5. Các thử nghiệm an toàn và bảo mật cho các mô đun nên được xuất phát từ các mối nguy hiểm có thể nhận dạng hoặc các mối nguy hiểm có thể lường trước theo trường hợp sử dụng dự kiến. Các mối nguy hiểm chưa được phát hiện có thể được thảo luận và ghi lại trong quá trình phân tích rủi ro. Các tiêu chuẩn an toàn rô bốt quốc tế cho các ứng dụng khác nhau có thể thiết lập các yêu cầu và biện pháp bảo vệ để giúp giảm rủi ro xuống mức có thể chấp nhận được đối với các tình huống nguy hiểm cụ thể (ví dụ: giới hạn an toàn). Các thử nghiệm về đặc tính và chức năng nên được thực hiện theo các nội dung tại Điều 6 và Điều 7.

Việc thử nghiệm có thể bao gồm (nhưng không giới hạn) các hạng mục dưới đây; một số các thử nghiệm được trình bày trong Điều D.3.

- An toàn cơ học
- Đặc tính cơ học
- An toàn điện và khả năng tương thích điện từ
- Đặc tính điện và điện từ
- Phần mềm liên quan đến an toàn
- Bảo mật

- Môi trường
- An toàn sinh học và hóa học
- Khả năng tương tác
- Khả năng hoán đổi
- Yếu tố con người và khả năng sử dụng HRI
- Tính năng và an toàn của phần mềm trí tuệ nhân tạo

D.3 Thử nghiệm sự tuân thủ an toàn và bảo mật

D.3.1 Tổng quan

An toàn là yêu cầu thiết yếu của một mô đun trong các ứng dụng liên quan đến an toàn. Các biện pháp bảo vệ người dùng khỏi bị tổn hại phải được xác nhận. Hoạt động an toàn của một mô đun phải được xác định thông qua phân tích rủi ro. Các thử nghiệm an toàn phải đưa ra được các bằng chứng cần thiết để hỗ trợ quy trình đánh giá rủi ro. Các phần sau đây cung cấp hướng dẫn và ví dụ để hỗ trợ việc phát triển thêm các thử nghiệm an toàn cho các mô đun rô bốt dịch vụ.

D.3.2 Thử nghiệm an toàn cơ học

Việc chỉ định các thông số cơ học, chẳng hạn như hình dạng, trọng lượng, tải trọng tối đa, trọng tâm, v.v..., là những vấn đề quan trọng mà các nhà sản xuất cần xem xét để đảm bảo an toàn cơ học. Một số tiêu chuẩn ISO trình bày các phương pháp để xây dựng các thử nghiệm về an toàn cơ học, ví dụ: ISO 12100:2010 và ISO 13482:2014 sử dụng đánh giá rủi ro để đạt được các yêu cầu về an toàn. ISO 12106:2017 quy định phương pháp thử nghiệm các mẫu biến dạng đơn trục dưới sự kiểm soát ứng suất ở biên độ không đổi, nhiệt độ đồng đều và tỷ lệ ứng suất cố định để xác định các đặc tính mỏi.

D.3.3 Thử nghiệm an toàn điện và khả năng tương thích điện từ

Dòng điện, điện áp, khoảng cách rò giữa các dây dẫn, năng lượng của sóng bức xạ, v.v..., là các thông số đo lường phổ biến để xác định mức độ an toàn điện của các mô đun. Các tiêu chí đã được thiết lập theo các tiêu chuẩn về an toàn điện và EMC (tương thích điện từ). Ví dụ, IEC 60204-1:2016 chỉ định các yêu cầu chung về an toàn của thiết bị điện, IEC 60990:2016 quy định các phương pháp đo lường cho dòng điện và loạt tiêu chuẩn IEC 61000 bao hàm các khía cạnh EMC.

D.3.4 Thử nghiệm phần mềm liên quan đến an toàn

ISO/IEC/IEEE 12207:2017 và ISO/IEC/IEEE 15288:2015 đã quy định các chu trình thực hiện để phát triển phần mềm. Để đáp ứng các mức tính năng liên quan đến an toàn bắt buộc, thử nghiệm phần mềm bao gồm các thử nghiệm dựa trên thông số kỹ thuật (ví dụ: phân vùng tương đương, cây phân loại, phân tích giá trị biên), các thử nghiệm dựa trên cấu trúc (ví dụ: thử câu lệnh, kiểm thử nhánh, kiểm thử quyết định) và các bài kiểm tra dựa trên kinh nghiệm (ví dụ: đoán lỗi). Bộ tiêu chuẩn ISO/IEC/IEEE 29119 quy định quy tắc, quy trình, tài liệu và kỹ thuật để thử nghiệm phần mềm.

D.3.5 Thử nghiệm bảo mật

ISO/IEC TS 3 0104:2015 mô tả các cơ chế bảo mật vật lý. Bên cạnh yếu tố vật lý, ISO/IEC 27001:2013 và ISO/IEC 27002:2013 còn chỉ định các yêu cầu về quản lý bảo mật và quy tắc thực hành cho các biện pháp kiểm soát bảo mật của không gian mạng được mô tả trong ISO/IEC 27032:2012. Loạt tiêu chuẩn ISO/IEC 15408 thiết lập các tiêu chí đánh giá cho bảo mật công nghệ thông tin, và loạt tiêu chuẩn ISO/IEC 19896 xác định các yêu cầu về năng lực đối với người thử nghiệm và người đánh giá. Các yêu cầu thử nghiệm đối với mô đun mật mã được mô tả trong JSO/IEC 24759:2017:

D.3.6 Thử nghiệm an toàn sinh học và hóa học

ISO 14123-1:2015 thiết lập các nguyên tắc để kiểm soát rủi ro đối với sức khỏe do các chất nguy hại phát ra từ máy móc. Bộ tiêu chuẩn ISO 10993 cung cấp các phương pháp đánh giá khả năng tương thích sinh học để xác định xem các yêu cầu về an toàn sinh học và hóa học có tuân thủ hay không.

D.4 Thử nghiệm sự tuân thủ tính năng

D.4.1 Tổng quan

Tính năng của mô đun phải được đo lường và kiểm tra để xác nhận rằng mô đun tuân thủ các yêu cầu được thiết kế. Mặc dù hầu hết các thông số đều có thể đo lường được bởi các nhà sản xuất, nhưng sự phù hợp với ISO/IEC 17025:2017 hoặc bộ quy tắc Thực hành phòng thí nghiệm tốt (GLP) của đơn vị đo lường cần được xem xét.

D.4.2 Thử nghiệm tính năng cơ học

Nhà sản xuất phải chỉ định một số thông số để xác định tính năng cơ học của một mô đun. Ví dụ, các đại lượng cơ học về khối lượng, tốc độ, lực, áp suất, v.v... Độ bền kết cấu là một trong các đặc điểm quan trọng của mô đun liên quan đến giới hạn về tính năng của nó. Luôn phải xem xét đặc điểm này trong mỗi tình huống áp dụng, đặc biệt là với kiểu ghép nối nối tiếp. Tính năng hoặc độ bền tổng thể bị giới hạn bởi các điểm hoặc mô đun yếu nhất trong chuỗi ghép nối đó. Trong kỹ thuật cơ khí, cần xem xét các lực và mô men tác động lên mô đun trong hệ trục tọa độ ba chiều, trong đó ứng suất tối đa, về nguyên tắc, không được vượt quá ứng suất giới hạn của vật liệu. Nhà sản xuất phải cung cấp thông tin về cơ học vật liệu thông qua thử nghiệm tính năng này cho khách hàng để đánh giá độ bền tổng thể trong các tình huống và các kết nối mô đun của họ.

Về tính năng của kết cấu, nhiều điều kiện khác nhau về lực và mô men có thể được áp dụng tùy theo ứng dụng hoặc tình huống có thể xảy ra, chẳng hạn như mô đun được sử dụng ở trạng thái chịu tải trọng tĩnh hoặc động.

Các thử nghiệm có thể xem xét:

- Lực và mô men tác động trên 1 đến 3 trục (trục đơn hoặc kết hợp)
- Lực và mô men tĩnh

- Lực và mô men động bao gồm cả các trạng thái va đập, tuần hoàn và thay đổi ngẫu nhiên.

Các thử nghiệm phải được thực hiện bằng đồng hồ đo lực đã hiệu chuẩn để đo lực và bộ chuyển đổi mô men xoắn đã hiệu chuẩn để xác định mô men xoắn. Các nhà sản xuất phải cung cấp đủ bằng chứng để làm tài liệu tham khảo cho khách hàng của họ.

D.4.3 Thử nghiệm tính năng điện và điện tử

Các mô đun điện và điện tử, ví dụ như pin, phát hiện và đo khoảng cách ánh sáng, truyền thông không dây cung cấp các chức năng riêng của chúng với các thông số kỹ thuật về điện dung, dòng điện, điện áp, tần số, cường độ, v.v... Các thông số điện và điện tử sẽ quyết định tính năng của mô đun.

Mô đun pin là nguồn điện của rô bốt dịch vụ và dung lượng của nó sẽ ảnh hưởng đáng kể đến thời gian hoạt động của các chức năng được hỗ trợ. Tiêu chuẩn IEC 60086-1:2015 được ban hành nhằm mục đích chuẩn hóa thông số kỹ thuật của pin chính.

Tần số và cường độ của ánh sáng phát hiện sẽ ảnh hưởng đến độ phân giải và độ nhạy của mô đun cảm biến. Loạt tiêu chuẩn ISO/TS 19159 quy định việc hiệu chuẩn và xác nhận cảm biến bằng nhiều kỹ thuật khác nhau. Các cảm biến nhạy điện không tiếp xúc có thể tham khảo IEC 61496-1:2012 để biết các yêu cầu chung về thiết kế.

Cường độ tín hiệu của mô đun không dây sẽ quyết định chất lượng truyền thông. Với các quy định về công nghệ thông tin và truyền thông có thể tham khảo loạt tiêu chuẩn ISO/IEC /JTC 1.

D.4.4 Thử nghiệm tính năng của phần mềm trí tuệ nhân tạo

Tính năng của phần mềm chung được định hình khi hoàn thành mã hóa, nhưng tính năng của trí tuệ nhân tạo (AI) có thể tiếp tục phát triển thông qua dữ liệu ngày càng tăng. Nếu mô đun đã được nhúng bằng AI, các nhà sản xuất có thể phải đánh giá liên tục và phân tích xem tính năng của nó có phù hợp với các yêu cầu được thiết kế hay không và liệu có gây ra bất kỳ mối lo ngại nào về an toàn không thể chấp nhận được hay không.

Một yếu tố quan trọng của AI là dữ liệu và ISO/IEC TR 20547-2:2018 cung cấp các ví dụ về các trường hợp sử dụng dữ liệu lớn cùng các yêu cầu kèm theo. Các tiêu chuẩn về AI vẫn đang được phát triển.

D.4.5 Thử nghiệm môi trường

Tình trạng của môi trường thường được mô tả bằng một thông số thống kê, chẳng hạn như nhiệt độ, độ ẩm, chất lượng không khí, v.v... Môi trường là một yếu tố quan trọng đối với chức năng và tuổi thọ của sản phẩm và các nhà sản xuất phải xác nhận xem mô đun có khả năng hoạt động trong môi trường dự định với tính năng đã nêu hay không.

IEC 60721-3-1:2018 phân loại các nhóm thông số môi trường và mức độ nghiêm trọng của chúng đối với sản phẩm, còn bộ tiêu chuẩn IEC 60068 mô tả các phương pháp thử nghiệm tương ứng với các điều kiện môi trường khác nhau. IEC 60529:2013 xác định các mức độ bảo vệ do vỏ bọc cung cấp cho thiết

bị điện để xác định mã IP. Nếu điều kiện môi trường thay đổi, các điều kiện mới phải được đưa vào các trường hợp thử nghiệm.

Do vật liệu khác nhau, các mô đun phải có các phương pháp gia tăng áp lực khác nhau để chạy thử nghiệm môi trường trong thời gian ngắn hơn. Ổ đĩa thể rắn (SSD) có thể được sử dụng làm mô đun lưu trữ cơ bản trong các rô bốt dịch vụ. Lấy SSD làm ví dụ, quá trình lão hóa của bộ nhớ flash NAND dựa trên SSD có thể được đẩy nhanh hơn với nhiệt độ cao hơn. Theo tiêu chuẩn JEDEC cho Yêu cầu về ổ đĩa thể rắn và Phương pháp thử độ bền, JESD 2188B.01, 6.1.3, Bảng 3, thử nghiệm lưu trữ dữ liệu ở 66 °C trong 96 giờ tương đương với việc lưu trữ ở 30 °C trong 1 năm.

D.4.6 Thử nghiệm về yếu tố con người và khả năng sử dụng

Các yếu tố con người và khả năng sử dụng là các đặc điểm của giao diện người dùng ảnh hưởng đến tương tác giữa người dùng và các mô đun. Các tương tác bao gồm các tiếp xúc vật lý, nhận thức thông tin và các quyết định kéo theo. Kỹ thuật về yếu tố con người và về khả năng sử dụng có nghĩa là thiết kế và phát triển giao diện người dùng thông qua việc áp dụng kiến thức về hành vi, khả năng, hạn chế và các đặc điểm khác của con người để tạo điều kiện thuận lợi cho việc sử dụng các mô đun. Việc đánh giá giao diện người dùng đã thiết kế được tiến hành như các thử nghiệm về yếu tố con người và khả năng sử dụng. *Các lỗi sử dụng có thể xảy ra và mức độ hài lòng của người dùng có thể được xác định* bằng những thử nghiệm này.

Lỗi sử dụng là hành động của người dùng (hoặc thiếu hành động) không tuân thủ kỳ vọng về thiết kế của nhà sản xuất và dẫn đến các tác vụ không hoàn thành. Hơn nữa, lỗi sử dụng có thể gây ra các mối nguy hiểm và gây hại cho người dùng và các mô đun. Ví dụ, việc ghép không thành công các đầu nối cơ và điện của các mô đun có thể phá vỡ cấu trúc vật lý và con người có thể bị điện giật. Nếu lỗi của người dùng liên quan đến tác hại nghiêm trọng, nhà sản xuất có thể cần xem xét các thử nghiệm về khả năng sử dụng như một phần của các yêu cầu về an toàn. Một giao diện người dùng được thiết kế tốt có thể đạt được các hành động chính xác của người dùng và ngăn ngừa các lỗi sử dụng có thể gây ra tác hại, ảnh hưởng trực tiếp đến sự hài lòng của người dùng và do đó thúc đẩy các giá trị của sản phẩm. Để có được bằng chứng về thiết kế tốt cho các yếu tố con người và khả năng sử dụng, các thử nghiệm xác nhận phải thu thập dữ liệu với sự nghiêm ngặt về mặt khoa học.

Các thử nghiệm về yếu tố con người và khả năng sử dụng được tiến hành để xác nhận thiết kế và chứng minh rằng các mô đun có thể được sử dụng bởi người dùng được nhắm đến với các mục đích đã định mà không có rủi ro không thể chấp nhận được. Một thử nghiệm có thể bao gồm:

- Giao diện người dùng thể hiện thiết kế của mô đun cần thử nghiệm
- Những người tham gia đại diện cho người dùng dự kiến
- Các tác vụ thể hiện các tình huống sử dụng để kiểm tra mô đun (Nhà sản xuất phải chỉ định tiêu chí đạt/không đạt)
- Các điều kiện thể hiện môi trường sử dụng thực tế

Thử nghiệm có thể được xử lý bằng cách quan sát tính năng vận hành tác vụ của những người tham gia, ghi lại các lỗi sử dụng xảy ra và phỏng vấn người tham gia về trải nghiệm sử dụng. Dữ liệu thu thập cần được phân tích để liên kết các bằng chứng và lập luận rằng mô đun tuân thủ với các thông số kỹ thuật về yếu tố con người và khả năng sử dụng do nhà sản xuất tuyên bố. ISO/TS 20282-2:2013 quy định phương pháp thử nghiệm tổng hợp dựa trên người dùng để đo lường khả năng sử dụng.

D.4.7 Kiểm tra và xác nhận

Có thể áp dụng quy trình kiểm tra và xác nhận để khẳng định rằng các mô đun phần cứng đáp ứng các yêu cầu của thông số kỹ thuật thiết kế và ứng dụng tương ứng. Các thông số kỹ thuật cần được mô tả theo các mẫu ở Phụ lục A, trong đó các giao diện liên quan đến cơ học, phần cứng, truyền thông, an toàn/bảo mật, đầu vào và đầu ra cần được chỉ định rõ ràng để tuân thủ các nguyên tắc cơ bản về khả năng hoán đổi, khả năng tương tác và độ chi tiết, v.v...

Cần áp dụng quy trình kiểm tra cho toàn bộ quá trình thiết kế và phát triển sản phẩm, ví dụ, phải sử dụng phương pháp hình thức trong giai đoạn thiết kế ý tưởng và phương pháp thử nghiệm của bên thứ ba cho giai đoạn thử nghiệm loại.

Cần chỉ định rõ ràng các trường hợp sử dụng và các thuộc tính chính tương ứng của mô đun phần cứng. Để xác nhận thêm xem mô đun có đáp ứng yêu cầu của ứng dụng hay không, cần sử dụng các phương pháp xác nhận liên quan. Ví dụ, mô đun chung cho sàn di động dùng trong lĩnh vực kho vận cần được xác nhận trong tình huống cụ thể ứng với các tiêu chuẩn đã công bố.

Thư mục tài liệu tham khảo

[1] TCVN 13228:2020 (ISO 8373:2012), *Rô bốt và các bộ phận cấu thành rô bốt – Từ vựng.*

[2] TCVN 13234 (ISO 9409-1), *Tay máy rô bốt công nghiệp – Mặt lắp ghép cơ khí – Phần 1: Dạng Tấm.*

[3] TCVN 13234 (ISO 9409-2), *Tay máy rô bốt công nghiệp – Mặt lắp ghép cơ khí – Phần 1: Dạng Trục.*

[4] TCVN 13229-1 (ISO 10218-1), *Rô bốt và các bộ phận cấu thành rô bốt – Yêu cầu an toàn cho rô bốt công nghiệp – Phần 1: Rô bốt.*

[5] TCVN 13229-2 (ISO 10218-2), *Rô bốt và các bộ phận cấu thành rô bốt – Yêu cầu an toàn cho rô bốt công nghiệp – Phần 2: Hệ thống rô bốt và sự tích hợp.*

[6] ISO 10303, *Industrialautomation systems and integration - Productdata representation and exchange (Hệ thống tự động hóa công nghiệp và tích hợp - Biểu diễn và trao đổi dữ liệu sản phẩm).*

[7] TCVN 7391 (ISO 10993), *Đánh giá sinh học trang thiết bị y tế.*

[8] TCVN 13230 (ISO 11593), *Rô bốt cho môi trường công nghiệp – Hế thống thay đổi tự động khâu tác động cuối – Từ vựng.*

[9] ISO 12106:2017, *Metallic materials - Fatigue testing - Axial-strain-controlled method (Vật liệu kim loại - Kiểm tra độ mỏi - Phương pháp kiểm soát biến dạng trục).*

[10] TCVN 13231 (ISO 13482), *Rô bốt và các bộ phận cấu thành rô bốt – Yêu cầu an toàn cho các rô bốt chăm sóc cá nhân.*

[11] ISO 13849-1, *Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (An toàn máy - Các bộ phận liên quan đến an toàn của hệ thống điều khiển - Phần 1: Nguyên tắc chung để thiết kế).*

[12] TCVN 6722-1:2000 (ISO 14123-1:2015), *An toàn máy – Giảm sự ảnh hưởng đối với sức khỏe do các chất nguy hiểm phát sinh từ máy – Phần 1: Nguyên tắc và uy định đối với nhà sản xuất.*

[13] TCVN 13700 (ISO/TS 15066), *Rô bốt và cơ cấu rô bốt – Rô bốt hợp tác.*

[14] ISO/TS 19159, *Geographic information - Calibration and validation of remote sensing imagery sensors and data (Thông tin địa lý - Hiệu chuẩn và xác thực dữ liệu và cảm biến hình ảnh từ xa).*

[15] TCVN 14446 (ISO 19649), *Rô bốt di động – Từ vựng.*

[16] TCVN 11698-2:2016 (ISO/TS 20282-2:2013), *Tính khả dụng của các sản phẩm tiêu dùng và các sản phẩm sử dụng công cộng – Phần 2: Phương pháp thử nghiệm tổng thể.*

[17] TCVN 9696-1 (ISO/IEC 7498-1), *Công nghệ thông tin – Liên kết hệ thống mở - Mô hình tham chiếu cơ sở - Phần 1: Mô hình cơ sở.*

[18] TCVN 8709 (ISO/IEC 15408), *Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin.*

[19] TCVN ISO/IEC 17025:2017 (ISO/IEC 17025:2017), *Yêu cầu chung về năng lực của các phòng thử nghiệm và hiệu chuẩn.*

[20] TCVN 13723 (ISO/IEC 19896), Kỹ thuật an toàn công nghệ thông tin – *Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin.*

[21] TCVN 13239-2:2020 (ISO/IEC TR 20547-2:2018), *Công nghệ thông tin – Kiến trúc tham chiếu dữ liệu lớp – Phần 2: Các trường hợp sử dụng và yêu cầu dẫn xuất.*

[22] ISO/IEC/CD 23053, *Framework for Artificial Intelligence (AI) Systems Using Machine Learning (Khung cho Hệ thống Trí tuệ nhân tạo (AI) Sử dụng Học máy).*

[23] TCVN 12211:2018 (ISO/IEC 24759:2017), *Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu kiểm thử cho mô đun mật mã.*

[24] TCVN ISO/IEC 27001 (ISO/IEC27100), *Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin- Các yêu cầu.*

[25] TCVN ISO/IEC 27002 (ISO:27002), *Công nghệ thông tin – Các kỹ thuật an toàn – Quy tắc thực hành quản lý an toàn thông tin.*

[26] ISO/IEC TS 30104:2015, *Information technology - Security techniques - Physical security attacks, mitigation techniques and security requirements (Công nghệ thông tin - Kỹ thuật bảo mật - Bảo mật vật lý các cuộc tấn công, kỹ thuật giảm thiểu và yêu cầu bảo mật).*

[27] ISO/IEC/IEEE 12207:2017, *Systems and software engineering- Software life cycle processes (Kỹ thuật hệ thống và phần mềm - Quy trình vòng đời phần mềm).*

[28] ISO/IEC/IEEE 15288, *Systems and software engineering- System life cycle processes (Kỹ thuật hệ thống và phần mềm - Quy trình vòng đời hệ thống).*

[29] TCVN 12849 (ISO/IEC/IEEE 29119) *(toàn bộ các phần).*

[30] TCVN 7699 (IEC 60068), *Thử nghiệm môi trường.*

[31] IEC 60086-1, *Primary batteries- Part 1: General (Pin sơ cấp – Phần 1: Tổng quan).*

[32] TCVN 12669-1 (IEC 60204-1), *Yêu cầu chung đối với thiết bị điện của máy.*

[33] TCVN 4255 (IEC 60529), *Cấp bảo vệ bằng vỏ ngoài (mã IP).*

[34] IEC/TR 60601-4-1, *Medical electrical equipment - Part 4-1: Guidance and interpretation - Medical electrical equipment and medical electrical systems employing a degree of autonomy (Thiết bị điện y tế - Phần 4-1: Hướng dẫn và giải thích - Thiết bị điện y tế và hệ thống điện y tế sử dụng một mức độ tự chủ).*

[35] TCVN 7921-3-1 (IEC 60721-3-1), *Phân loại điều kiện môi trường – Phần 3-1: Phân loại theo nhóm các tham số môi trường và độ khắc nghiệt – Bảo quản.*

[36] IEC 60990, *Methods of measurement of touch current and protective conductor current (Phương pháp đo dòng điện tiếp xúc và dòng điện bảo vệ).*

[37] TCVN 7909 (IEC 61000), *Tương thích điện từ (EMC).*

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

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

[40] IEC 61784-3:2016, *Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions (Mạng truyền thông công nghiệp - Hồ sơ - Phần 3: Bus trường an toàn chức năng - Quy tắc chung và định nghĩa hồ sơ).*

[41] IEC 61800-5-2, *Adjustable speed electrical power drive systems- Part 5-2: Safety requirements Functional (Hệ thống truyền động điện có tốc độ điều chỉnh - Phần 5-2: Yêu cầu an toàn Chức năng).*

[42] IEC 62061, *Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems (An toàn máy móc - An toàn chức năng của các hệ thống điều khiển điện, điện tử và điện tử có thể lập trình liên quan đến an toàn).*

[43] TCVN 13340 (IEC 62280), *Ứng dụng đường sắt - Hệ thống thông tin liên lạc, tín hiệu và xử lý - Thông tin liên quan đến an toàn trong hệ thống truyền dẫn.*

[44] IEC/TR 62390, *Common automation device - Profile guideline (Thiết bị tự động hóa chung- Hướng dẫn hồ sơ).*

[45] IEC 62443, *Industrial communication networks - Network and system security (Mạng truyền thông công nghiệp - Bảo mật mạng và hệ thống).*

[46] IEC/TR 63074, ED1, *Security aspects related to functional safety of safety - related control systems (Các khía cạnh an ninh liên quan đến an toàn chức năng của các hệ thống kiểm soát liên quan đến an toàn).*

[47] ITU-T F.747.3 *Requirements and functional model for a ubiquitous network robot platform that supports ubiquitous sensor network applications and services, 2013 (Yêu cầu và mô hình chức năng cho nền tảng robot mạng phổ biến hỗ trợ các ứng dụng và dịch vụ mạng cảm biến phổ biến, 2013).*

[48] NIST SP 800-37 Rev. 1, *Guide for applying the risk management framework to Federal information systems: a security life cycle approach (Hướng dẫn áp dụng khuôn khổ quản lý rủi ro cho hệ thống thông tin liên bang: phương pháp tiếp cận vòng đời bảo mật).*

[49] VIRK GS, CLAWAR *Modularity for robotic systems, International journal of Robotics Research, Vol 22, Issue 3-4, pp265-277, 2003 (tính mô đun cho các hệ thống rô bốt, Tạp chí quốc tế về nghiên cứu rô bốt, Tập 22, Số 3-4, trang 265-277, 2003).*

[50] NORMAN P *Modularity - The degree to which a system's components may be separated and combined, Ross Robotics, 2017 (Tính mô-đun - Mức độ mà các thành phần của hệ thống có thể được tách biệt và kết hợp, Ross Robotics, 2017).*

[51] BROOKS RA, *A robust layered control system for a mobile robot, IEEE journal of Robotics and Automation, Volume 2 (1), 1986 (BROOKS RA, Hệ thống điều khiển nhiều lớp mạnh mẽ cho rô bốt di động, Tạp chí IEEE về Robot và Tự động hóa, Tập 2 (1), 1986).*

[52] *OMG HARDWARE ABSTRACTION LAYER FOR ROBOTIC TECHNOLOGY https://www.omg.org/spec/HAL4RT/ (OMG LỚP TRÍCH DẪN PHẦN CỨNG CHO CÔNG NGHỆ ROBOT https://www.omg.org/spec/HAL4RT/).*

[53] *OMG Robotic Localisation Service vl.l, 2012 (Dịch vụ địa phương hóa rô bốt vl.l, 2012).*

[54] *OMG Robotic interaction service framework (ROISTM), v 1.2, 2018 (Dịch vụ tương tác khung rô bốt (ROISTM), v 1.2, 2018).*