



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẢNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)
CỤC SỞ HỮU TRÍ TUỆ

(11)



1-0024401

(51)⁷ G06F 9/445

(13) B

(21) 1-2016-03824

(22) 11/03/2015

(86) PCT/CN2015/074003 11/03/2015

(87) WO2015/143989A1 01/10/2015

(30) 201410114837.9 25/03/2014 CN

(45) 27/07/2020 388

(43) 26/12/2016 345A

(73) 1. HUAWEI TECHNOLOGIES CO., LTD. (CN)

Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China

2. WUHAN UNIVERSITY (CN)

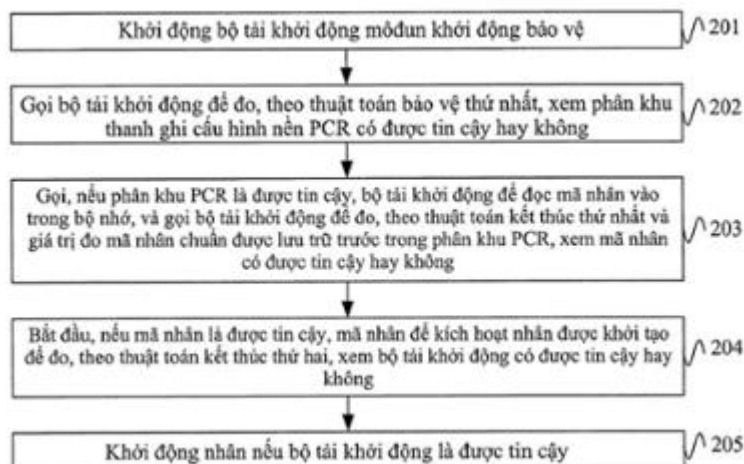
Luoja Hill, Wuchang District Wuhan, Hubei 430072, China

(72) LI, Zhi (CN); ZHAO, Bo (CN); FEI, Yongkang (CN).

(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ KHỞI ĐỘNG NHÂN HỆ ĐIỀU HÀNH TIN CẬY

(57) Sáng chế đề cập đến phương pháp và thiết bị khởi động nhân hệ điều hành tin cậy. Trong đó phương pháp bao gồm các bước: khởi động bộ nạp khởi động môđun khởi động bảo vệ (201); gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không (202); nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân có được tin cậy hay không (203); khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không (204); và khởi động nhân nếu bộ nạp khởi động là được tin cậy (205). Độ an toàn khởi động nhân được nâng cao.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực về công nghệ tính toán tin cậy, và cụ thể là, đến phương pháp và thiết bị khởi động nhân hệ điều hành tin cậy.

Tình trạng kỹ thuật của sáng chế

Trong những năm gần đây, với việc phổ biến của mạng truyền thông di động thế hệ thứ ba (3rd Generation, 3G), các điện thoại thông minh đã trở thành các sản phẩm công nghệ thông tin phát triển nhanh nhất (công nghệ thông tin-IT).

Các thiết bị di động thông minh phát triển nhanh mang lại kỷ nguyên thông tin thành đỉnh cao phát triển mới. Tuy nhiên, các nhu cầu vượt quá đã xảy ra về việc nâng cao hiệu suất ứng dụng của các thiết bị điện thoại thông minh, và sự phát triển về hiệu quả bảo vệ bị bỏ qua, kết quả là sự phát triển về hiệu quả bảo vệ của các thiết bị di động bị tụt hậu, và vấn đề bảo vệ tiềm năng của các điện thoại di động ngày càng lộ rõ. Đối với việc khởi động an toàn các thiết bị điện thoại thông minh, trong kỹ thuật đã biết, phương pháp thực hiện khởi động từ bộ bảo vệ bên ngoài, nghĩa là, bộ bảo vệ bên ngoài được kết nối đến thiết bị cài đặt bằng cách sử dụng giao diện truyền thông, để cung cấp chức năng an toàn cho thiết bị cài đặt. Khi thiết bị được khởi động, thiết bị cài đặt đầu tiên cần xác định sự có mặt của bộ bảo vệ bên ngoài, để ngăn ngừa việc khởi động không được phép từ bỏ qua sự khởi động bên ngoài của sự tin cậy của chuỗi tin cậy, chương trình khởi động hệ thống sau đó được tải, chương trình khởi động gọi bộ phận bảo vệ để thực hiện phép đo đồng nhất trên nhân của hệ điều hành, và sau khi xác nhận thành công, nhân được khởi động.

Tuy nhiên, phương pháp được sử dụng trong kỹ thuật đã biết có nhược điểm sau: Bộ bảo vệ bên ngoài cần phải truyền thông với thiết bị điện thoại thông minh bằng cách sử dụng giao diện bên ngoài, và đầu cuối truyền thông di động thông thường không cung cấp giao diện bên ngoài như vậy, và do đó phạm vi ứng dụng của phương pháp được sử dụng trong kỹ thuật đã biết bị hạn chế.

Thứ hai, theo giải pháp khởi động, nhân có thể được khởi động miễn là sự có mặt của bộ bảo vệ bên ngoài được xác nhận trước khi khởi động được thực hiện. Do đó, theo giải pháp này, có thể là việc khởi động không được phép bỏ qua bộ phận bảo vệ là tương đối cao, và độ an toàn khởi động nhân là tương đối thấp.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp và thiết bị khởi động nhân hệ điều hành tin cậy, mà được sử dụng để nâng cao độ an toàn khởi động nhân.

Theo khía cạnh thứ nhất, một phương án của sáng chế đề xuất phương pháp khởi động nhân hệ điều hành tin cậy, bao gồm các bước:

khởi động bộ nạp khởi động môđun khởi động bảo vệ;

gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không;

gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân hệ điều hành vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không;

khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân hệ điều hành để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và

khởi động nhân nếu bộ nạp khởi động là được tin cậy.

Dựa vào khía cạnh thứ nhất, trong cách thực hiện có thể thứ nhất của khía cạnh thứ nhất, phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV; và

việc gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không bao gồm các bước:

gọi bộ nạp khởi động để tính giá trị đo thực phân khu PCR theo thuật toán bảo vệ thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực phân khu

PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có được tin cậy hay không, trong đó nếu giá trị đo thực phân khu PCR bằng giá trị đo chuẩn phân khu PCR, phân khu PCR là được tin cậy.

Dựa vào cách thực hiện có thể thứ nhất của khía cạnh thứ nhất, trong cách thực hiện có thể thứ hai của khía cạnh thứ nhất, việc thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV bao gồm các bước:

 tạo ra khóa gốc dựa vào PIN được đưa vào bởi người dùng; và

 giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu ENC, của phân khu PCR.

Dựa vào khía cạnh thứ nhất hoặc cách thực hiện có thể thứ nhất hoặc thứ hai của khía cạnh thứ nhất, trong cách thực hiện có thể thứ ba của khía cạnh thứ nhất, phương pháp còn bao gồm các bước:

 thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR; và

 việc gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân hệ điều hành vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không bao gồm các bước:

 nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân hệ điều hành vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân hệ điều hành theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã nhân hệ điều hành có bằng giá trị đo mã nhân hệ điều hành chuẩn hay không, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân bằng giá trị đo mã nhân hệ điều hành chuẩn, mã nhân hệ điều hành là được tin cậy.

Dựa vào khía cạnh thứ nhất hoặc cách thực hiện bất kỳ trong số các cách thực hiện có thể từ thứ nhất đến thứ ba của khía cạnh thứ nhất, trong cách thực hiện có thể thứ tư của khía cạnh thứ nhất, phương pháp còn bao gồm các

bước:

thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và

khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không bao gồm các bước:

nếu mã nhân hệ điều hành là được tin cậy, khởi tạo mã nhân để kích hoạt nhân được khởi tạo để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn bộ nạp khởi động hay không, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, bộ nạp khởi động là được tin cậy.

Dựa vào khía cạnh thứ nhất hoặc cách bắt kỳ trong các cách thực hiện có thể thứ nhất đến thứ tư của khía cạnh thứ nhất, trong cách thực hiện có thể thứ năm của khía cạnh thứ nhất, sau việc khởi động nhân, phương pháp còn bao gồm các bước:

gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Dựa vào cách thực hiện có thể thứ năm của khía cạnh thứ nhất, trong cách thực hiện có thể thứ sáu của khía cạnh thứ nhất, phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

việc gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không bao gồm các bước:

gọi nhân để tính giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo

thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân hay không, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Dựa vào cách thực hiện có thể thứ nhất hoặc thứ sáu của khía cạnh thứ nhất, trong cách thực hiện có thể thứ bảy của khía cạnh thứ nhất, sau việc khởi động hệ điều hành, phương pháp còn bao gồm các bước:

gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

Dựa vào cách thực hiện có thể thứ bảy của khía cạnh thứ nhất, trong cách thực hiện có thể thứ tám của khía cạnh thứ nhất, phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng; và

việc gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không bao gồm các bước:

gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn của chương trình ứng dụng hay không, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, chương trình ứng dụng là được tin cậy.

Theo khía cạnh thứ hai, một phương án của sáng chế đề xuất phương pháp khởi động nhân hệ điều hành tin cậy khác, bao gồm các bước:

khởi động bộ nạp khởi động môđun khởi động bảo vệ;

gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không;

gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; và

nếu mã nhân hệ điều hành là được tin cậy, chạy mã nhân hệ điều hành để khởi động nhân.

Dựa vào khía cạnh thứ hai, trong cách thực hiện có thể thứ nhất của khía cạnh thứ hai, sau việc chạy mã nhân hệ điều hành để khởi động nhân, phương pháp còn bao gồm các bước:

gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không;

nếu bộ nạp khởi động là được tin cậy, gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Dựa vào khía cạnh thứ hai hoặc cách thực hiện có thể thứ nhất của khía cạnh thứ hai, trong cách thực hiện có thể thứ hai của khía cạnh thứ hai, phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV; và

việc gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không bao gồm các bước:

gọi bộ nạp khởi động để tính giá trị đo thực phân khu PCR theo thuật toán bảo vệ thứ nhất được lưu trữ trước, và đo, bằng cách so sánh xem giá trị đo thực phân khu PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có được tin cậy hay không, trong đó nếu giá trị đo thực phân khu

PCR bằng giá trị đo chuẩn phân khu PCR, phân khu PCR là được tin cậy.

Dựa vào cách thực hiện có thể thứ hai của khía cạnh thứ hai, trong cách thực hiện có thể thứ ba của khía cạnh thứ hai, việc thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV bao gồm các bước:

tạo ra khóa gốc dựa vào PIN được đưa vào bởi người dùng; và

giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu ENV, của phân khu PCR.

Dựa vào khía cạnh thứ hai hoặc cách thực hiện bất kỳ trong các cách thực hiện có thể từ thứ nhất đến thứ ba của khía cạnh thứ hai, trong cách thực hiện có thể thứ tư của khía cạnh thứ hai, phương pháp còn bao gồm các bước:

thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR; và

việc gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không bao gồm các bước:

nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã nhân có bằng giá trị đo mã nhân hệ điều hành chuẩn hay không, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân bằng giá trị đo mã nhân hệ điều hành chuẩn, mã nhân hệ điều hành là được tin cậy.

Dựa vào cách thực hiện bất kỳ trong các cách thực hiện có thể thứ nhất đến thứ tư của khía cạnh thứ hai, trong cách thực hiện có thể thứ năm của khía cạnh thứ hai, phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và

việc gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không bao gồm các bước:

gọi nhân để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn bộ nạp khởi động hay không, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, bộ nạp khởi động là được tin cậy.

Dựa vào cách thực hiện bất kỳ trong các cách thực hiện có thể thứ nhất đến thứ năm của khía cạnh thứ hai, trong cách thực hiện có thể thứ sáu của khía cạnh thứ hai, phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

việc gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không bao gồm các bước:

gọi nhân để tính giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân hay không, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Dựa vào cách thực hiện bất kỳ trong các cách thực hiện có thể thứ nhất đến thứ sáu của khía cạnh thứ hai, trong cách thực hiện có thể thứ bảy của khía cạnh thứ hai, sau việc khởi động hệ điều hành, phương pháp còn bao gồm các bước:

gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

khởi động chương trình ứng dụng nếu chương trình ứng dụng là được

tin cậy.

Dựa vào cách thực hiện có thể thứ bảy của khía cạnh thứ hai, trong cách thực hiện có thể thứ tám của khía cạnh thứ hai, phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng; và

việc gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không bao gồm các bước:

gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn của chương trình ứng dụng hay không, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, chương trình ứng dụng là được tin cậy.

Theo khía cạnh thứ ba, một phương án của sáng chế đề xuất thiết bị khởi động nhân hệ điều hành tin cậy, bao gồm:

môđun bắt đầu quá trình khởi động, được tạo cấu hình để khởi động bộ nạp khởi động môđun khởi động bảo vệ;

môđun đo thứ nhất, được tạo cấu hình để gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không, trong đó

môđun đo thứ nhất còn được tạo cấu hình để gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không;

môđun đo thứ hai, được tạo cấu hình để khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và

môđun khởi động nhân, được tạo cấu hình để khởi động nhân nếu bộ nạp khởi động là được tin cậy.

Dựa vào khía cạnh thứ ba, trong cách thực hiện có thể thứ nhất của khía cạnh thứ ba, thiết bị ngoài ra còn bao gồm:

môđun thu thập, được tạo cấu hình để thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV, trong đó

môđun đo thứ nhất được tạo cấu hình một cách đặc biệt để gọi bộ nạp khởi động để tính giá trị đo thực phân khu PCR theo thuật toán bảo vệ thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực phân khu PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có được tin cậy hay không, trong đó nếu giá trị đo thực phân khu PCR bằng giá trị đo chuẩn phân khu PCR, xác định được rằng phân khu PCR là được tin cậy.

Dựa vào cách thực hiện có thể thứ nhất của khía cạnh thứ ba, trong cách thực hiện có thể thứ hai của khía cạnh thứ ba, môđun thu thập được tạo cấu hình một cách đặc biệt để tạo ra khóa gốc dựa vào PIN được đưa vào bởi người dùng, và giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu ENC, của phân khu PCR.

Dựa vào khía cạnh thứ ba hoặc cách thực hiện có thể thứ nhất hoặc thứ hai của khía cạnh thứ ba, trong cách thực hiện có thể thứ ba của khía cạnh thứ ba,

môđun thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn mà được lưu trữ trước trong phân khu PCR, của mã nhân; và

môđun đo thứ nhất được tạo cấu hình một cách đặc biệt để: nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã nhân có bằng giá trị đo mã nhân hệ điều hành chuẩn hay không, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân bằng giá trị đo mã nhân hệ điều hành chuẩn, mã nhân hệ điều hành là được tin cậy.

Dựa vào khía cạnh thứ ba hoặc cách thực hiện bất kỳ trong số các cách

thực hiện có thể từ thứ nhất đến thứ ba của khía cạnh thứ ba, trong cách thực hiện có thể thứ tư của khía cạnh thứ ba,

môđun thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và

môđun đo thứ hai được tạo cấu hình một cách đặc biệt để: nếu mã nhân hệ điều hành là được tin cậy, khởi tạo mã nhân để kích hoạt nhân được khởi tạo để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn bộ nạp khởi động hay không, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, bộ nạp khởi động là được tin cậy.

Dựa vào khía cạnh thứ ba hoặc cách bất kỳ trong số các cách thực hiện có thể thứ nhất đến thứ tư của khía cạnh thứ ba, trong cách thực hiện có thể thứ năm của khía cạnh thứ ba, thiết bị ngoài ra còn bao gồm môđun khởi động hệ thống, trong đó

môđun đo thứ hai còn được tạo cấu hình để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

môđun khởi động hệ thống được tạo cấu hình để khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Dựa vào cách thực hiện có thể thứ năm của khía cạnh thứ ba, trong cách thực hiện có thể thứ sáu của khía cạnh thứ ba,

môđun thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

môđun đo thứ hai được tạo cấu hình một cách đặc biệt để gọi nhân để tính giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân hay không, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin

cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Dựa vào cách thực hiện có thể thứ nhất hoặc thứ sáu của khía cạnh thứ ba, trong cách thực hiện có thể thứ bảy của khía cạnh thứ ba, thiết bị ngoài ra còn bao gồm:

môđun đo thứ ba, được tạo cấu hình để gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

môđun khởi động chương trình ứng dụng, được tạo cấu hình để khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

Dựa vào cách thực hiện có thể thứ bảy của khía cạnh thứ ba, trong cách thực hiện có thể thứ tám của khía cạnh thứ ba,

môđun thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng; và

môđun đo thứ ba được tạo cấu hình một cách đặc biệt để gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn của chương trình ứng dụng hay không, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, chương trình ứng dụng là được tin cậy.

Theo khía cạnh thứ tư, một phương án của sáng chế đề xuất thiết bị khởi động nhân hệ điều hành tin cậy khác, bao gồm:

bộ bắt đầu quá trình khởi động, được tạo cấu hình để khởi động bộ nạp khởi động môđun khởi động bảo vệ;

bộ đo thứ nhất, được tạo cấu hình để gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không, trong đó

bộ đo thứ nhất còn được tạo cấu hình để gọi, nếu phân khu PCR là

được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; và

bộ khởi động nhân, được tạo cấu hình để: nếu mã nhân hệ điều hành là được tin cậy, chạy mã nhân hệ điều hành để khởi động nhân.

Dựa vào khía cạnh thứ tư, trong cách thực hiện có thể thứ nhất của khía cạnh thứ tư, thiết bị ngoài ra còn bao gồm:

bộ đo thứ hai, được tạo cấu hình để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không, trong đó

bộ đo thứ hai còn được tạo cấu hình để: nếu bộ nạp khởi động là được tin cậy, gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

bộ khởi động hệ thống, được tạo cấu hình để khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Dựa vào khía cạnh thứ tư hoặc cách thực hiện có thể thứ nhất của khía cạnh thứ tư, trong cách thực hiện có thể thứ hai của khía cạnh thứ tư, thiết bị ngoài ra còn bao gồm:

bộ phận thu thập, được tạo cấu hình để thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV, trong đó

bộ đo thứ nhất được tạo cấu hình một cách đặc biệt để gọi bộ nạp khởi động để tính giá trị đo thực phân khu PCR theo thuật toán bảo vệ thứ nhất được lưu trữ trước, và đo, bằng cách so sánh xem giá trị đo thực phân khu PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có được tin cậy hay không, trong đó nếu giá trị đo thực phân khu PCR bằng giá trị đo chuẩn phân khu PCR, phân khu PCR là được tin cậy.

Dựa vào cách thực hiện có thể thứ hai của khía cạnh thứ tư, trong cách thực hiện có thể thứ ba của khía cạnh thứ tư,

bộ phận thu thập được tạo cấu hình một cách đặc biệt để tạo ra khóa

gốc dựa vào PIN được đưa vào bởi người dùng, và giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu ENC, của phân khu PCR.

Dựa vào khía cạnh thứ tư hoặc các thực hiện bất kỳ trong số các cách thực hiện có thể từ thứ nhất đến thứ ba của khía cạnh thứ tư, trong cách thực hiện có thể thứ tư của khía cạnh thứ tư,

bộ phận thu thập còn được tạo cấu hình để thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR; và

bộ đo thứ nhất được tạo cấu hình một cách đặc biệt để: nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã nhân có bằng giá trị đo mã nhân hệ điều hành chuẩn hay không, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân bằng giá trị đo mã nhân hệ điều hành chuẩn, mã nhân hệ điều hành là được tin cậy.

Dựa vào các thực hiện bất kỳ trong các cách thực hiện có thể thứ nhất đến thứ tư của khía cạnh thứ tư, trong cách thực hiện có thể thứ năm của khía cạnh thứ tư,

bộ phận thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và

bộ đo thứ hai được tạo cấu hình một cách đặc biệt để gọi nhân để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn bộ nạp khởi động hay không, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, bộ nạp khởi động là được tin cậy.

Dựa vào cách thực hiện bất kỳ trong các cách thực hiện có thể thứ nhất đến thứ năm của khía cạnh thứ tư, trong cách thực hiện có thể thứ sáu của khía cạnh thứ tư,

bộ phận thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn

môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

bộ đo thứ hai được tạo cấu hình một cách đặc biệt để gọi nhân để tính giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân hay không, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Dựa vào các cách thực hiện có thể thứ nhất đến thứ sáu của khía cạnh thứ tư, trong cách thực hiện có thể thứ bảy của khía cạnh thứ tư, thiết bị ngoài ra còn bao gồm:

bộ đo thứ ba, được tạo cấu hình để gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

bộ phận khởi động chương trình ứng dụng, được tạo cấu hình để khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

Dựa vào cách thực hiện có thể thứ bảy của khía cạnh thứ tư, trong cách thực hiện có thể thứ tám của khía cạnh thứ tư,

bộ đo thứ ba được tạo cấu hình một cách đặc biệt để gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn của chương trình ứng dụng hay không, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, chương trình ứng dụng là được tin cậy.

Có thể thấy rằng, theo phương pháp và thiết bị khởi động nhân hệ điều hành tin cậy mà được đề xuất trong các phương án của sáng chế, bộ nạp khởi động môđun khởi động bảo vệ đầu tiên được gọi để đo xem phân khu thanh ghi

cấu hình nền (PCR) có được tin cậy hay không; sau khi xác định được rằng phân khu PCR là được tin cậy, bộ nạp khởi động được gọi để đo, theo thuật toán kết thúc thứ nhất và giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của mã nhân, xem mã nhân hệ điều hành có được tin cậy hay không; sau khi xác định được rằng mã nhân hệ điều hành là được tin cậy, mã nhân sau đó được khởi tạo để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và sau khi xác định được rằng bộ nạp khởi động là được tin cậy, nhân được khởi động. Nghĩa là, theo các giải pháp kỹ thuật được đề xuất trong sáng chế, nhân có thể được khởi động một cách an toàn chỉ khi bộ nạp khởi động mô đun khởi động bảo vệ, phân khu thanh ghi cấu hình nền (PCR), và mã nhân đều được tin cậy, độ tin cậy của mã nhân được đo bởi bộ nạp khởi động theo giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, và mã nhân được khởi tạo để kích hoạt nhân hệ điều hành để đo độ tin cậy của bộ nạp khởi động. Do đó, các giải pháp kỹ thuật được đề xuất trong các phương án của sáng chế có thể nâng cao độ an toàn khởi động nhân đến một mức nào đó.

Mô tả vắn tắt các hình vẽ

Để mô tả các giải pháp kỹ thuật trong các phương án của sáng chế hoặc trong giải pháp kỹ thuật đã biết một cách rõ ràng hơn, phần dưới đây mô tả vắn tắt các hình vẽ kèm theo cần để mô tả các phương án hoặc kỹ thuật đã biết. Rõ ràng là, các hình vẽ kèm theo trong phần mô tả dưới đây chỉ thể hiện một vài phương án của sáng chế, và người có trình độ trung bình trong lĩnh vực kỹ thuật tương ứng có thể vẫn có được các hình vẽ khác từ các hình vẽ kèm theo này mà không cần nỗ lực sáng tạo.

Fig.1 là lưu đồ để khởi động hệ thống theo sáng chế;

Fig.2a là lưu đồ của một phương án của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.2b là lưu đồ của phương án khác của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.2c là lưu đồ của phương án khác nữa của phương pháp khởi động nhân hệ

điều hành tin cậy theo sáng chế;

Fig.2d là lưu đồ của phương án khác nữa của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.3a là lưu đồ của phương án khác nữa của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.3b là lưu đồ của phương án khác nữa của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.3c là lưu đồ của phương án khác nữa của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.3d là lưu đồ của phương án khác nữa của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.4a là sơ đồ cấu trúc của một phương án của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.4b là sơ đồ cấu trúc của phương án khác của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.4c là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.4d là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.4e là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.4f là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.5a là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.5b là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.5c là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế;

Fig.5d là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ

điều hành tin cậy theo sáng chế;

Fig.5e là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế; và

Fig.5f là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế.

Mô tả chi tiết sáng chế

Phần dưới đây mô tả đầy đủ và rõ ràng các giải pháp kỹ thuật trong các phương án của sáng chế dựa vào các hình vẽ kèm theo trong các phương án của sáng chế. Rõ ràng là, các phương án được mô tả chỉ là một vài mà không phải tất cả các phương án của sáng chế. Tất cả các phương án khác thu được bởi người có trình độ trung bình trong lĩnh vực kỹ thuật tương ứng dựa vào các phương án của sáng chế mà không có sự nỗ lực sáng tạo vẫn sẽ nằm trong phạm vi bảo hộ của sáng chế.

Fig.1 là lưu đồ để khởi động hệ thống theo một phương án của sáng chế. Dựa vào phương pháp khởi động nhân hệ điều hành tin cậy được đề xuất trong các phương án được thể hiện trong sáng chế, qua sự so sánh, sự khác nhau giữa sơ đồ cấu trúc được thể hiện trong phương án này và thủ tục hệ thống được cài đặt trong kỹ thuật đã biết nằm ở chỗ: môđun nền thành phần mềm được tin cậy được thiết đặt bổ sung trong thủ tục khởi động hệ thống được cài đặt hiện thời. Môđun nền thành phần mềm được tin cậy có thể điều khiển việc thực hiện quy trình xử lý trong đó bộ nạp khởi động đo phân khu PCR và nhân, phép đo bộ nạp khởi động và môđun nâng cao việc quản lý bảo vệ nhân bởi nhân, và phép đo chương trình ứng dụng bởi môđun nâng cao việc quản lý bảo vệ nhân, trong đó các quy trình xử lý này nằm trong các phương pháp được thể hiện trên Fig.2.

Thủ tục khởi động hệ thống được tóm tắt là: Sau khi hệ thống được cấp nguồn, chương trình khởi động bảo vệ, nghĩa là, bộ nạp khởi động được khởi động, và môđun nền thành phần mềm được tin cậy gọi bộ nạp khởi động để đo phân khu thanh ghi định vị nền PCR. Nếu phân khu hiện thời PCR là được tin cậy, môđun nền thành phần mềm được tin cậy tiếp tục gọi bộ nạp khởi động

để đo nhân. Nếu nhân hiện thời là được tin cậy, môđun nền thành phần mềm được tin cậy chỉ dẫn bộ nạp khởi động tải nhân và khởi tạo nhân, và sau đó gọi nhân được khởi tạo để đo lại bộ nạp khởi động. Nếu bộ nạp khởi động là được tin cậy trong trường hợp này, môđun nền thành phần mềm được tin cậy chỉ dẫn nhân khởi động, và đo môđun nâng cao việc quản lý bảo vệ nhân. Nếu phép đo môđun nâng cao được đo việc quản lý bảo vệ nhân hiện được tin cậy, môđun nền thành phần mềm được tin cậy chỉ dẫn nhân tải môđun nâng cao việc quản lý bảo vệ nhân, và sau đó đo, bằng cách sử dụng môđun nâng cao việc quản lý bảo vệ nhân, chương trình ứng dụng cần được khởi động. Nếu kết quả đo được tin cậy, chương trình ứng dụng được khởi động bình thường. Bộ nạp khởi động đo phân khu PCR và nhân tương ứng theo thuật toán bảo vệ thứ nhất và thuật toán kết thúc thứ nhất bằng cách sử dụng môđun đo thứ nhất. Nhân đo bộ nạp khởi động và môđun nâng cao quản lý nhân một cách tương ứng theo thuật toán kết thúc thứ hai và thuật toán kết thúc thứ ba bằng cách sử dụng môđun đo thứ hai. Môđun nâng cao quản lý nhân đo chương trình ứng dụng theo thuật toán kết thúc thứ tư bằng cách sử dụng môđun đo thứ ba. Việc khởi động an toàn hệ thống cài đặt được tin cậy có thể được thực hiện bằng cách sử dụng phương pháp như vậy để thực hiện khởi động từng mức sau khi thực hiện phép đo từng mức.

Fig.2a là lưu đồ của một phương án của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế. Như được thể hiện trên Fig.2a, phương pháp khởi động nhân hệ điều hành tin cậy cụ thể bao gồm các bước:

S201: Khởi động bộ nạp khởi động môđun khởi động bảo vệ.

Hiện nay, hệ thống được cài đặt được sử dụng trong thiết bị đầu cuối, chẳng hạn như PC, điện thoại di động, hoặc iPad, chủ yếu bao gồm các môđun chức năng sau: chương trình khởi động (bộ nạp khởi động), nhân (Nhân), và môđun quản lý toàn nhân. Sau khi các môđun chức năng trong hệ thống được cài đặt được khởi động bình thường, người dùng có thể gọi các chương trình ứng dụng khác nhau để thực hiện các thao tác tương ứng.

Trong phương án này, sau khi thiết bị đầu cuối được cấp nguồn, nhằm

khởi động các môđun chức năng: môđun khởi động bảo vệ (bộ nạp khởi động) được lưu trữ trong bộ lưu trữ đầu tiên được tải vào trong hệ thống được cài đặt trong thiết bị để khởi động bộ nạp khởi động. Cụ thể là, trong phương án này, quy trình kết thúc khởi động bộ nạp khởi động được chia thành ba phần: phần BL 0 (bộ nạp khởi động 0), phần BL 1 (bộ nạp khởi động 1), và phần BL 2 (bộ nạp khởi động 2).

BL 0 đề cập đến mã khởi động được cài đặt trong iROM của S5PV210. Khi hệ thống vừa được cấp nguồn, toàn bộ trạng thái hệ thống không được khởi tạo, và đồng hồ bên trong không được thiết đặt. Trong trường hợp này, chỉ iRAM là thích hợp. Nếu nguồn cấp cấp nguồn bình thường trong trường hợp này, thủ tục khởi động sẽ khởi động từ mã khởi động được cài đặt trong iROM. Mã khởi động được cài đặt trong iROM là mã liên quan đến phần cứng. Nói chung, mã khởi động được cài đặt trong thiết bị phần cứng tương ứng trong cách thức phần cứng, mà không thể được thay đổi bởi người dùng. Mã khởi động chịu trách nhiệm khởi tạo đồng hồ của hệ thống, thiết đặt cảnh vệ, khởi tạo khối xếp và bó, và tải BL 1.

BL 1 đề cập đến mã của 16 K thứ nhất (tối đa là 16 K) của tệp nhị phân uboot.bin mà được sao chép tự động từ bộ lưu trữ ex-patulous (nand/sd/usb) bởi iRAM. Vai trò của BL 1 là phát hiện và khởi tạo RAM ngoại vi, đóng Cache, thiết đặt bó, và tải BL 2.

BL 2 đề cập đến mã uboot hoàn thiện được thực hiện trong bộ nhớ sau khi đổi hướng mã, và cũng được đề cập đến là bộ nạp khởi động chính. Bộ nạp khởi động chính mã là rất quan trọng, bao gồm khởi tạo hệ thống tệp, hỗ trợ mạng, khởi tạo bộ nhớ phụ, và công việc khác, và chịu trách nhiệm tải hệ điều hành (OS) nhân (mà sau đây được gọi ngắn gọn là nhân).

Quy trình kết thúc để khởi động bộ nạp khởi động có thể được mô tả như sau: Sau khi được khởi động, BL 0 (mã khởi động được cài đặt trong iROM) tải BL 1 (mã của 16 K thứ nhất B của bộ nạp khởi động) đến iRAM. Sau đó, BL 1 chạy trong iRAM và tải BL 2 (bộ nạp khởi động còn lại) đến bộ nhớ (SDRAM); và BL 2 tải nhân, và cho phép OS chạy trong SDRAM, sao cho OS

cuối cùng chạy trong SDRAM.

Việc khởi động bộ nạp khởi động môđun khởi động bảo vệ trong bước này đề cập đến khởi động phần BL 0 và phần BL 1 mà là trong bộ nạp khởi động sau khi hệ thống được cấp nguồn và bộ nạp khởi động trong bộ lưu trữ được tải.

S202: Gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không.

Trong phương án này, sau khi hệ thống khởi động phần BL 0 và phần BL 1 mà ở trong bộ nạp khởi động, và trước khi hệ thống thực hiện phần BL 2, nghĩa là, tải nhân, hệ thống chỉ dẫn bộ nạp khởi động đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không. Các thông số liên quan, chẳng hạn như các giá trị đo chuẩn được sử dụng để đo tính toàn vẹn hoặc độ an toàn của các nút, cần thiết bởi các nút (chẳng hạn như bộ nạp khởi động, nhân, và môđun nâng cao việc quản lý bảo vệ nhân) trong quy trình khởi động hệ thống được lưu trữ trước trong phân khu PCR. Các giá trị đo chuẩn này có thể được chủ động báo cáo bởi các nút đến hệ thống trong quy trình khởi động hệ thống cho thời điểm thứ nhất, và các hệ thống lưu trữ giá trị đo chuẩn trong bộ phận lưu trữ đặc biệt trong hệ thống.

Cụ thể là, thuật toán bảo vệ thứ nhất có thể được đóng gói và được lưu trữ trong bộ phận lưu trữ trong hệ thống. Sau khi bộ nạp khởi động hoàn tất thực hiện quy trình xử lý BL 1, bộ nạp khởi động có thể kích hoạt việc nhắc nhở hệ thống rằng quy trình xử lý BL 1 hiện thời đã hoàn tất. Sau khi nhận tín hiệu khởi động, hệ thống gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất được lưu trữ trước trong bộ phận lưu trữ, độ tin cậy của phân khu thanh ghi cấu hình nền (PCR).

Cụ thể là, thuật toán bảo vệ thứ nhất có thể cụ thể là, ví dụ như, thuật toán dữ liệu hồng bảo vệ (sha1) hoặc thuật toán dữ liệu SM3 dân dụng, và nguyên tắc đo thuật toán bảo vệ thứ nhất có thể được mô tả như sau: việc tính toán được thực hiện trên đối tượng cần được đo, ví dụ như, tập tin ảnh, bằng cách sử dụng hai thuật toán nêu trên, để thu được giá trị đo (nghĩa là, giá trị phân loại của đối tượng được đo, trong đó giá trị phân loại của đối tượng được đo

tương ứng với thuật toán sha1 là 160 bit, và giá trị phân loại của đối tượng được đo tương ứng với thuật toán SM3 là 256 bit) của đối tượng được đo hiện thời, trong đó giá trị đo là giá trị duy nhất, mà thu được qua việc tính toán bằng cách sử dụng thuật toán tương ứng, của đối tượng được đo. Nếu giá trị đo của đối tượng được đo thay đổi, có thể coi rằng đối tượng được đo đã được thay đổi hoặc đã được cải biến. Tương tự như vậy, quy trình xử lý trong đó bộ nạp khởi động đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không được mô tả như sau: Bộ nạp khởi động đọc, đối với đối tượng được đo, tập tin ảnh của phân khu PCR vào trong bộ nhớ, và tính toán giá trị đo của phân khu PCR bằng cách sử dụng thuật toán bảo vệ thứ nhất, trong đó nếu giá trị đo không thay đổi, nó chỉ báo rằng phân khu PCR không thay đổi, và là an toàn và được tin cậy. Ngược lại, nếu giá trị đo thay đổi, nó chỉ báo rằng phân khu PCR có thể đã được cải biến nhân tạo và thay đổi; trong trường hợp này, độ an toàn của dữ liệu liên quan được lưu trữ trong phân khu PCR cũng cần phải xem lại. Để đảm bảo an toàn môi trường chạy của toàn bộ hệ thống, bộ nạp khởi động thông báo hệ thống rằng việc đo độ an toàn PCR thất bại, và nhắc nhở hệ thống ngừng quy trình khởi động hệ thống và tắt thiết bị.

Thuật toán bảo vệ thứ nhất được sử dụng trong quy trình xử lý để đo thực độ tin cậy của phân khu PCR có thể còn là thuật toán bất kỳ trong số thuật toán MTV5, thuật toán SHA2, thuật toán SHA256, và thuật toán MD. Phương pháp và nguyên tắc đo độ tin cậy của thuật toán bảo vệ thứ nhất là giống như đối với sha1 và SM3, chỉ có các quy trình xử lý tính toán cụ thể khác nhau cho các loại thuật toán cụ thể khác nhau. Theo mức hiểu của người có trình độ trung bình trong lĩnh vực, dựa vào cùng một nguyên tắc, độ tin cậy của phân khu PCR được đo bằng cách sử dụng phương pháp được đề cập ở trên, và các chi tiết sẽ không được mô tả sau đây một lần nữa.

S203: Gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước

trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không.

Cụ thể là, khi giá trị đo của phân khu PCR được tính toán bằng cách sử dụng thuật toán bảo vệ thứ nhất, sau khi được xác định theo giá trị đo rằng phân khu PCR là được tin cậy, hệ thống gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, sử dụng mã nhân làm đối tượng được đo, và xác định, bằng cách gọi bộ nạp khởi động khớp và tính toán, theo thuật toán kết thúc thứ nhất được lưu trữ trước trong bộ phận lưu trữ, mối tương quan giá trị giữa giá trị đo thực mã nhân và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không. Thuật toán kết thúc thứ nhất có thể một trong số các thuật toán bảo vệ thứ nhất được liệt kê bước 202, và đối với phương pháp và nguyên tắc để đo độ tin cậy của mã nhân bởi bộ nạp khởi động theo thuật toán kết thúc thứ nhất, có thể thực hiện tham chiếu theo nội dung của quy trình đo độ tin cậy của phân khu PCR theo thuật toán bảo vệ thứ nhất trong bước 202, và các chi tiết sẽ không được mô tả sau đây một lần nữa.

S204: Khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không.

Cụ thể là, sau khi thuật toán kết thúc thứ nhất được sử dụng để đo mà mã nhân được đảm bảo và được tin cậy, hệ thống gọi bộ nạp khởi động để thực hiện quy trình xử lý BL 2 đến tải nhân. Ở trạng thái sớm của việc tải nhân, mã nhân để tải đầu tiên cần phải được khởi tạo. Khác với kỹ thuật đã biết, trong phương án này của sáng chế, sau khi hoàn tất việc khởi động mã nhân, hệ thống đầu tiên khởi động nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; thuật toán kết thúc thứ hai, giống như thuật toán kết thúc thứ nhất, cũng được lưu trữ trước trong bộ phận lưu trữ trong hệ thống, và loại thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ hai có thể giống với loại thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ nhất, hoặc thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ hai có thể là thuật toán bất kỳ trong số các thuật toán

được liệt kê ở trên; và quy trình tính cụ thể của thuật toán kết thúc thứ hai là cũng giống như đối với phương pháp và nguyên tắc để đo độ tin cậy của mã nhân bằng cách sử dụng thuật toán kết thúc thứ nhất, và các chi tiết sẽ không được mô tả sau đây một lần nữa trong phương án này. Ngược lại, nếu thuật toán kết thúc thứ nhất được sử dụng để đo rằng mã nhân là không được tin cậy, bộ nạp khởi động thông báo hệ thống rằng việc đo độ an toàn nhân hệ thống thất bại, và nhắc nhở hệ thống ngừng quy trình khởi động hệ thống và tắt thiết bị.

S205: Khởi động nhân nếu bộ nạp khởi động là được tin cậy.

Cụ thể là, sau khi nhân được khởi tạo sử dụng thuật toán kết thúc thứ hai để đo bộ nạp khởi động là được tin cậy, hệ thống hoàn tất khởi động mã nhân và cho phép OS chạy trong SDRAM, sao cho OS cuối cùng chạy trong SDRAM. Ngược lại, nếu nhân được khởi tạo sử dụng thuật toán kết thúc thứ hai để đo mà bộ nạp khởi động là không được tin cậy, nhân thông báo hệ thống rằng việc đo độ an toàn bộ nạp khởi động thất bại, và nhắc nhở hệ thống ngừng quy trình khởi động hệ thống và tắt thiết bị.

Theo phương pháp khởi động nhân hệ điều hành tin cậy được đề xuất theo sáng chế, bộ nạp khởi động môđun khởi động bảo vệ được khởi động; bộ nạp khởi động được gọi để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không; nếu phân khu PCR là được tin cậy, bộ nạp khởi động được gọi để đọc mã nhân vào trong bộ nhớ, và bộ nạp khởi động được gọi để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; nếu mã nhân hệ điều hành là được tin cậy, mã nhân được khởi tạo để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và nếu bộ nạp khởi động là được tin cậy, nhân được khởi động. Theo giải pháp này, độ an toàn khởi động nhân được nâng cao đến một mức nào đó.

Fig.2b là lưu đồ của phương án khác của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế. Phương pháp khởi động nhân hệ điều hành tin cậy trong phương án này là cách thực hiện cụ thể của phương án được thể

hiện trên Fig.2a. Như được thể hiện trên Fig.2b, phương pháp khởi động nhân hệ điều hành tin cậy cụ thể bao gồm các bước:

S211: Khởi động bộ nạp khởi động môđun khởi động bảo vệ. Đối với quy trình cụ thể để thực hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 201.

S212: Thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu môi trường ENV, của phân khu PCR.

Trước khi bước 202 trong phương án được thể hiện trên Fig.2a, hệ thống có thể trước tiên còn thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu môi trường ENV, của phân khu PCR, trong đó giá trị đo chuẩn là giá trị đo nghĩa là được tạo ra, bằng cách tính toán, bằng cách sử dụng thuật toán bảo vệ thứ nhất, khi phân khu PCR lưu trữ cho thời điểm thứ nhất các thông số liên quan cần thiết bởi các nút khi hệ thống được khởi động, tập tin ảnh mà tương ứng với phân khu hiện thời PCR.

Cụ thể là, quy trình cụ thể của việc thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu môi trường ENV, của phân khu PCR là như sau đây:

1. Tạo ra khóa gốc dựa vào PIN được đưa vào bởi người dùng.

Khi hệ thống được cấp nguồn và chạy cho thời điểm thứ nhất, hệ thống đầu tiên nhận các giá trị đo chuẩn mà được gửi bởi các nút khóa chẳng hạn như bộ nạp khởi động và nhân trong hệ thống và mà được sử dụng để đo độ an toàn của các nút khóa; sau đó, các giá trị đo chuẩn được lưu trữ trong phân khu PCR trong thiết bị lưu trữ, để làm tham chiếu đo trong tương lai. Sau đó, hệ thống sử dụng thuật toán bảo vệ thứ nhất để tính giá trị đo chuẩn P (20 Bytes) của tập tin ảnh mà tương ứng với phân khu PCR, trong đó giá trị đo chuẩn được mã hóa bằng cách sử dụng khóa khởi động thiết bị SRK để tạo ra $ENC\{P\}$, và $ENC\{P\}$ được lưu trữ ở 20 byte cuối cùng của phân khu ENV. Khóa gốc được tạo ra bởi người dùng; và mỗi lần hệ thống được khởi động, người dùng có thể đưa ra nhân khóa khởi động tương ứng, nghĩa là, PIN, sao cho hệ thống tạo ra khóa gốc.

2. Giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá

trị đo chuẩn, mà được lưu trữ trước trong phân khu ENV, của phân khu PCR.

Sau khi bộ nạp khởi động hoàn tất quy trình xử lý BL 1, hệ thống thu PIN được đưa vào bởi người dùng, và tạo ra SRK theo PIN, sao cho việc giải mã được thực hiện ở 20 byte cuối cùng của phân khu ENV.

Nếu PIN được đưa vào bởi người dùng là chính xác, hệ thống tạo ra SRK theo PIN, sao cho có thể được thực hiện rằng $ENC\{P\}$ trong phân khu ENV được giải mã thành công, và giá trị P được thu. Giá trị P là giá trị đo chuẩn tương ứng với phân khu PCR. Xem phân khu PCR có được tin cậy hay không có thể được xác định bằng cách so sánh P và giá trị đo thực phân khu PCR. Theo cách này, ngay cả nếu người dùng không được phép chen thông tin bất kỳ trong phân khu PCR, người dùng không được phép vẫn không thể chen $ENC\{P\}$ tương ứng. Do đó, ngay khi phân khu PCR bị chen, trường hợp này có thể được phát hiện, và hệ thống còn ngay lập tức dừng quy trình khởi động hiện thời.

S213: Gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không. Đối với quy trình xử lý cụ thể để thực hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 202.

Cụ thể là, quy trình xử lý cụ thể trong đó bộ nạp khởi động đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không có thể là như sau đây: Đầu tiên, thuật toán bảo vệ thứ nhất được sử dụng để tính tập tin ảnh của đối tượng được đo, nghĩa là, phân khu PCR, để thu được giá trị đo thực của phân khu hiện thời PCR. Bộ nạp khởi động xác định, bằng cách so sánh xem giá trị đo thực phân khu PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có thay đổi trong hai lần đo hay không, để xác định xem phân khu PCR có được tin cậy hay không. Nếu giá trị đo thực phân khu PCR bằng giá trị đo chuẩn phân khu PCR, nó chỉ báo rằng phân khu PCR không thay đổi, và môi trường của phân khu PCR được đảm bảo và được tin cậy.

S214: Thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR.

Trước khi bước 203 trong phương án được thể hiện trên Fig.2a, hệ thống có thể còn đầu tiên thu thập giá trị đo mã nhân hệ điều hành chuẩn từ phân khu PCR, trong đó giá trị đo chuẩn được chủ động báo cáo bởi nhân đến hệ thống, khi hệ thống được khởi động cho thời điểm thứ nhất, sau khi nhân tính toán, theo thuật toán kết thúc thứ nhất, giá trị chuẩn tương ứng với nhân, và được lưu trữ trong phân khu PCR bởi hệ thống.

S215: Gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không. Đối với quy trình xử lý cụ thể để thực hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 203.

Cụ thể là, nếu phân khu PCR là được tin cậy, hệ thống gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã nhân có bằng giá trị đo chuẩn hay không, mà được thu được từ phân khu PCR, của mã nhân, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân bằng giá trị đo mã nhân hệ điều hành chuẩn, nó chỉ báo rằng mã nhân hệ điều hành là được tin cậy.

S216: Thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR.

Trước khi bước 204 trong phương án được thể hiện trên Fig.2a, hệ thống có thể còn đầu tiên thu thập giá trị đo chuẩn bộ nạp khởi động từ phân khu PCR, trong đó giá trị đo chuẩn được chủ động báo cáo bởi bộ nạp khởi động đến hệ thống, khi hệ thống được khởi động cho thời điểm thứ nhất, sau khi bộ nạp khởi động tính toán, theo thuật toán kết thúc thứ hai, giá trị chuẩn tương ứng với bộ nạp khởi động, và được lưu trữ trong phân khu PCR bởi hệ thống.

S217: Khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không. Đối với quy trình xử lý cụ thể để thực

hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 204.

Cụ thể là, nếu mã nhân hệ điều hành là được tin cậy, hệ thống đầu tiên khởi tạo mã nhân để kích hoạt nhân được khởi tạo để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn hay không, mà được thu được từ phân khu PCR, của bộ nạp khởi động, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, nó chỉ báo rằng bộ nạp khởi động là được tin cậy.

S218: Khởi động nhân nếu bộ nạp khởi động là được tin cậy. Đối với quy trình xử lý cụ thể để thực hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 105.

Theo phương pháp khởi động nhân hệ điều hành tin cậy được đề xuất theo sáng chế, bộ nạp khởi động môđun khởi động bảo vệ được khởi động; bộ nạp khởi động được gọi để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không; nếu phân khu PCR là được tin cậy, bộ nạp khởi động được gọi để đọc mã nhân vào trong bộ nhớ, và bộ nạp khởi động được gọi để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; nếu mã nhân hệ điều hành là được tin cậy, mã nhân được khởi tạo để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và nếu bộ nạp khởi động là được tin cậy, nhân được khởi động. Theo giải pháp này, độ an toàn khởi động nhân được nâng cao đến một mức nào đó.

Fig.2c là lưu đồ của phương án khác nữa của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế. Phương pháp khởi động nhân hệ điều hành tin cậy trong phương án này là cách thực hiện cụ thể của phương án được thể hiện trên Fig.2a. Như được thể hiện trên Fig.2c, đối với nội dung của các bước từ 221 đến 225, có thể thực hiện tham chiếu theo nội dung của các bước từ 201 đến 205, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Trong phương án này, dựa vào phương pháp được thể hiện trên Fig.2a, sau khi bước

205, phương pháp khởi động nhân hệ điều hành tin cậy ngoài ra còn bao gồm các bước:

S226: Gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không.

Thuật toán kết thúc thứ ba, giống như thuật toán kết thúc thứ nhất, cũng được lưu trữ trước trong bộ phận lưu trữ trong hệ thống, và loại thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ ba có thể giống với loại thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ nhất, hoặc thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ ba là thuật toán bất kỳ trong số các thuật toán được liệt kê ở trên; và quy trình đo cụ thể thuật toán kết thúc thứ ba cũng giống như phương pháp và nguyên tắc để đo độ tin cậy của mã nhân bằng cách sử dụng thuật toán kết thúc thứ nhất, và các chi tiết sẽ không được mô tả sau đây một lần nữa trong phương án này.

Cụ thể là, sau khi khởi động nhân được toàn tất, hệ thống có thể tiếp tục để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không.

Phương pháp đo cụ thể là: hệ thống đầu tiên thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân từ phân khu PCR, trong đó giá trị đo chuẩn được chủ động báo cáo bởi môđun nâng cao việc quản lý bảo vệ nhân đến hệ thống, khi hệ thống được khởi động cho thời điểm thứ nhất, sau khi môđun nâng cao việc quản lý bảo vệ nhân sử dụng tập tin ảnh tương ứng với môđun nâng cao việc quản lý bảo vệ nhân làm đối tượng được đo và tính toán, theo thuật toán kết thúc thứ ba, giá trị chuẩn tương ứng với môđun nâng cao việc quản lý bảo vệ nhân, và được lưu trữ trong phân khu PCR bởi hệ thống.

Ngoài ra, hệ thống gọi nhân để tính giá trị đo thực hiện thời môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn hay không, được thu thập từ phân khu PCR, của môđun nâng cao việc quản lý bảo vệ nhân, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao

việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, nó chỉ báo rằng môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

S227: Khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Khi môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy, nhân tải động môđun nâng cao việc quản lý bảo vệ nhân, và khởi động toàn bộ hệ thống, mà bao gồm tất cả các trương trình cần thiết để chạy trong môi trường làm việc bình thường của hệ thống.

Hơn nữa, như được thể hiện trên Fig.2d, sau khi bước 227, nghĩa là, sau khi hệ điều hành hoàn tất khởi động bình thường, và trước khi hệ điều hành khởi động mỗi chương trình ứng dụng, hệ điều hành có thể còn thực hiện các bước sau đây (S238 và S239) để đảm bảo thêm độ an toàn của hệ điều hành. Như được thể hiện trên Fig.2d, đối với nội dung của các bước từ 231 đến 237, có thể thực hiện tham chiếu theo nội dung của các bước từ 221 đến 227, và các chi tiết sẽ không được mô tả sau đây một lần nữa.

S238: Gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không.

Thuật toán kết thúc thứ tư, giống như thuật toán kết thúc thứ nhất, cũng được lưu trữ trước trong bộ phận lưu trữ trong hệ thống, và loại thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ tư có thể có thể là giống như loại thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ nhất, hoặc thuật toán mà được tham chiếu cụ thể bởi thuật toán kết thúc thứ tư có thể là thuật toán bất kỳ trong số các thuật toán được liệt kê ở trên; và quy trình tính cụ thể của thuật toán kết thúc thứ tư là cũng giống như đối với phương pháp và nguyên tắc để đo độ tin cậy của mã nhân bằng cách sử dụng thuật toán kết thúc thứ nhất, và các chi tiết sẽ không được mô tả sau đây một lần nữa trong phương án này.

Phương pháp đo cụ thể là: hệ thống đầu tiên thu thập, từ phân khu

PCR, giá trị đo chuẩn của chương trình ứng dụng cần được khởi động, trong đó giá trị đo chuẩn được chủ động báo cáo đến hệ thống, khi chương trình ứng dụng tương ứng được khởi động cho thời điểm thứ nhất, sau khi hệ thống gọi môđun nâng cao việc quản lý bảo vệ nhân để sử dụng tập tin ảnh tương ứng với chương trình ứng dụng làm đối tượng được đo và tính toán, theo thuật toán kết thúc thứ tư, giá trị chuẩn tương ứng với chương trình ứng dụng, và được lưu trữ trong phân khu PCR bởi hệ thống.

Ngoài ra, hệ thống gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực hiện thời của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn hay không, được thu thập từ phân khu PCR, của chương trình ứng dụng, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, nó chỉ báo rằng chương trình ứng dụng là được tin cậy.

S239: Nếu chương trình ứng dụng là được tin cậy, hệ thống khởi động chương trình ứng dụng. Ngược lại, nếu giá trị đo thực của chương trình ứng dụng không bằng giá trị đo chuẩn của chương trình ứng dụng, nó chỉ báo rằng chương trình ứng dụng là không được tin cậy; trong trường hợp này, môđun nâng cao việc quản lý bảo vệ nhân chủ động thông báo hệ thống rằng chương trình ứng dụng hiện thời cần được khởi động là không được tin cậy, và yêu cầu chỉ dẫn xem có tiếp tục thực hiện khởi động hay không. Sau đó, người dùng xác định xem có tiếp tục thực hiện khởi động theo cách bật cửa sổ thông tin tương ứng bởi hệ thống hay không.

Có thể hiểu rằng bước 236 và bước 237 hoặc các bước từ 236 đến 239 trong phương án này có thể cũng được thực hiện sau khi bước 218 trong phương án được thể hiện trên Fig.2b, và các chi tiết sẽ không được mô tả sau đây một lần nữa.

Theo phương pháp khởi động nhân hệ điều hành tin cậy được đề xuất theo sáng chế, bộ nạp khởi động môđun khởi động bảo vệ được khởi động; bộ nạp khởi động được gọi để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu

thanh ghi cấu hình nền (PCR) có được tin cậy hay không; nếu phân khu PCR là được tin cậy, bộ nạp khởi động được gọi để đọc mã nhân vào trong bộ nhớ, và bộ nạp khởi động được gọi để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; nếu mã nhân hệ điều hành là được tin cậy, mã nhân được khởi tạo để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; nếu bộ nạp khởi động là được tin cậy, nhân được khởi động; nhân được gọi để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy, hệ điều hành được khởi động. Theo giải pháp này, độ an toàn khởi động nhân và độ an toàn khởi động hệ điều hành được nâng cao đến một mức nào đó.

Fig.3a là lưu đồ của phương án khác của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế. Như được thể hiện trên Fig.3a, phương pháp khởi động nhân hệ điều hành tin cậy cụ thể bao gồm các bước:

S301: Khởi động bộ nạp khởi động môđun khởi động bảo vệ. Đối với quy trình xử lý cụ thể để thực hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 201.

S302: Gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không. Đối với quy trình xử lý cụ thể để thực hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 202.

S303: Gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không. Đối với quy trình xử lý cụ thể để thực hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 203.

S304: Nếu mã nhân hệ điều hành là được tin cậy, chạy mã nhân hệ

điều hành để khởi động nhân.

Cụ thể là, khi bộ nạp khởi động được gọi để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, rằng mã nhân hệ điều hành là được tin cậy, hệ thống hoàn tất khởi động mã nhân và cho phép OS chạy trong SDRAM, sao cho OS cuối cùng chạy trong SDRAM. Ngược lại, nếu bộ nạp khởi động được gọi để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, rằng mã nhân là không được tin cậy, bộ nạp khởi động thông báo hệ thống rằng việc đo độ an toàn nhân thất bại, và nhắc nhở hệ thống ngừng quy trình khởi động hệ thống và tắt thiết bị.

Trong phương pháp khởi động nhân hệ điều hành tin cậy được thể hiện trong phương án này, so sánh với với phương án được thể hiện trên Fig.2a, rằng nhân đo bộ nạp khởi động một lần nữa trong quy trình khởi động bị loại bỏ, và toàn bộ nhân được khởi động trực tiếp, điều này làm đơn giản hóa quy trình xử lý nhân đến một mức nào đó. Độ an toàn khi nhân được khởi động cũng được nâng cao bằng việc đo độ an toàn của phân khu PCR trước khi nhân được tải.

Fig.3b là lưu đồ của phương án khác của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế. Phương pháp khởi động nhân hệ điều hành tin cậy trong phương án này là cách thực hiện cụ thể của phương án được thể hiện trên Fig.3a. Như được thể hiện trên Fig.3b, phương pháp khởi động nhân hệ điều hành tin cậy cụ thể bao gồm các bước:

S311: Khởi động bộ nạp khởi động môđun khởi động bảo vệ.

S312: Thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu môi trường ENV, của phân khu PCR.

S313: Gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không.

S314: Thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR.

S315: Gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán

kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không.

S316: Nếu mã nhân hệ điều hành là được tin cậy, chạy mã nhân hệ điều hành để khởi động nhân.

Đối với quy trình cụ thể để thực hiện các bước từ 311 đến 315, có thể thực hiện tham chiếu theo nội dung của các bước từ 211 đến 215, và đối với quy trình cụ thể để thực hiện bước 316, có thể thực hiện tham chiếu theo nội dung của bước 304; các chi tiết sẽ không được mô tả sau đây một lần nữa.

Trong phương pháp khởi động nhân hệ điều hành tin cậy được thể hiện trong phương án này, khi được so sánh với phương án được thể hiện trên Fig.2b, rằng nhân đo bộ nạp khởi động một lần nữa trong quy trình khởi động được loại bỏ, và toàn bộ nhân được khởi động trực tiếp, điều này làm đơn giản hóa quy trình nhân đến một mức nào đó. Độ an toàn khi nhân được khởi động cũng được nâng cao bằng cách đo độ an toàn của phân khu PCR trước khi nhân được tải.

Fig.3c là lưu đồ của phương án khác nữa của phương pháp khởi động nhân hệ điều hành tin cậy theo sáng chế. Phương pháp khởi động nhân hệ điều hành tin cậy trong phương án này là cách thực hiện cụ thể của phương án được thể hiện trên Fig.3a. Như được thể hiện trên Fig.3c, dựa vào phương pháp được thể hiện trên Fig.3a, sau khi bước 304, phương pháp khởi động nhân hệ điều hành tin cậy ngoài ra còn bao gồm các bước:

S325: Gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không.

S326: Nếu bộ nạp khởi động là được tin cậy, gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không.

S327: Khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Như được thể hiện trên Fig.3c, đối với nội dung của các bước từ 321 đến 324, có thể thực hiện tham chiếu theo nội dung của các bước từ 301 đến 304, và các chi tiết sẽ không được mô tả sau đây một lần nữa.

Hơn nữa, như được thể hiện trên Fig.3d, trong phương án này, sau khi bước 327, nghĩa là, sau khi hệ điều hành hoàn tất khởi động bình thường, và trước khi hệ điều hành khởi động từng chương trình ứng dụng, hệ điều hành có thể còn thực hiện các bước sau đây (S338 và S339) để đảm bảo hơn nữa độ an toàn của hệ điều hành.

S338: Gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không.

S339: Hệ thống khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

Đối với quy trình xử lý cụ thể để thực hiện bước 338 và bước 339, có thể thực hiện tham chiếu theo nội dung của bước 238 và bước 239.

Có thể hiểu rằng bước 336 và bước 337 hoặc các bước từ 336 đến 339 trong phương án này có thể cũng được thực hiện sau khi bước 316 trong phương án này được thể hiện trên Fig.3b, và các chi tiết sẽ không được mô tả sau đây một lần nữa.

Hơn nữa, trước khi bước 335, phương pháp có thể ngoài ra còn bao gồm các bước: thu thập giá trị đo chuẩn, mà được sắp trước trong phân khu PCR, của bộ nạp khởi động. Đối với quy trình xử lý cụ thể để thực hiện bước này, có thể thực hiện tham chiếu theo nội dung của bước 216.

Hơn nữa, đối với quy trình xử lý cụ thể để thực hiện bước 335, có thể thực hiện tham chiếu theo nội dung của bước 217.

Trong phương pháp khởi động nhân hệ điều hành tin cậy được thể hiện trong phương án này, được so sánh với với phương án được thể hiện trên Fig.2c, rằng nhân đo bộ nạp khởi động một lần nữa trong quy trình khởi động được loại bỏ, và toàn bộ nhân được khởi động trực tiếp; sau đó, nhân được khởi động được gọi để thực hiện phép đo độ an toàn trên bộ nạp khởi động, mà đơn giản hóa thủ tục khởi động nhân đến một mức nào đó, và đảm bảo hệ điều hành khởi động một cách an toàn.

Người có trình độ trung bình trong lĩnh vực kỹ thuật tương ứng có thể

hiểu rằng toàn bộ hoặc một số các bước của phương pháp các phương án có thể được thực hiện bởi chương trình chỉ dẫn phần cứng liên quan. Chương trình có thể được lưu trữ trong phương tiện lưu trữ đọc được bởi máy tính. Khi chương trình chạy, các bước của phương pháp các phương án được thực hiện. Phương tiện lưu trữ nên trên bao gồm: phương tiện bất kỳ mà có thể lưu trữ mã chương trình, chẳng hạn như ROM, RAM, đĩa từ, hoặc đĩa quang.

Fig.4a là sơ đồ cấu trúc của một phương án của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế. Thiết bị có thể là thống khởi động được gắn hoặc môđun chức năng cố định được thêm mới vào hệ thống, ví dụ như, môđun nền thành phần mềm được tin cậy được thể hiện trên Fig.1. Thiết bị khởi động nhân hệ điều hành tin cậy có thể thực hiện phương pháp khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.2. Như được thể hiện trên Fig.4, thiết bị khởi động nhân hệ điều hành tin cậy cụ thể bao gồm: môđun bắt đầu quá trình khởi động 401, môđun đo thứ nhất 402, môđun đo thứ hai 403, và môđun khởi động nhân 404, trong đó

môđun bắt đầu quá trình khởi động 401 được tạo cấu hình để khởi động bộ nạp khởi động môđun khởi động bảo vệ;

môđun đo thứ nhất 402 được tạo cấu hình để gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không, trong đó

môđun đo thứ nhất 402 còn được tạo cấu hình để gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không;

môđun đo thứ hai 403 được tạo cấu hình để khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và

môđun khởi động nhân 404 được tạo cấu hình để khởi động nhân nếu bộ nạp khởi động là được tin cậy.

Hơn nữa, như được thể hiện trên Fig.4b, các chức năng cụ thể của 411 đến 414 là giống như các chức năng tương ứng của 401 đến 404 trên Fig.4a, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này có thể ngoài ra còn bao gồm môđun thu thập 415, trong đó môđun thu thập 415 được tạo cấu hình để:

thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV; thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR; và thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR, trong đó trong phương án được thể hiện trên Fig.4b, Các bước phương pháp của phương án được thể hiện trên Fig.2b có thể được thực hiện bởi thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.4b.

Hơn nữa, như được thể hiện trên Fig.4c, các chức năng cụ thể của 421 đến 424 là giống như các chức năng tương ứng của 401 đến 404 trên Fig.4a, và sẽ không được mô tả ở đây một lần nữa. Trong thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này:

môđun đo thứ hai 423 còn được tạo cấu hình để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

như được thể hiện trên Fig.4c, thiết bị khởi động nhân hệ điều hành tin cậy có thể ngoài ra còn bao gồm môđun khởi động hệ thống 426, được tạo cấu hình để khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Các bước phương pháp của phương án được thể hiện trên Fig.2c có thể được thực hiện bởi thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.4c.

Hơn nữa, như được thể hiện trên Fig.4d, các chức năng cụ thể của 431 đến 434 và 436 là giống như các chức năng tương ứng của 421 đến 424 và 426 trên Fig.4c, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này có thể

ngoài ra còn bao gồm:

môđun đo thứ ba 437, được tạo cấu hình để gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

môđun khởi động chương trình ứng dụng 438, được tạo cấu hình để khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

Các bước phương pháp của phương án được thể hiện trên Fig.2d có thể được thực hiện bởi thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.4d.

Hơn nữa, như được thể hiện trên Fig.4e, các chức năng cụ thể của 441 đến 445 là giống như các chức năng tương ứng của 411 đến 415 trên Fig.4b, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Trong thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này:

môđun đo thứ hai 443 còn được tạo cấu hình để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

môđun thu thập 445 còn được tạo cấu hình để thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

như được thể hiện trên Fig.4e, thiết bị khởi động nhân hệ điều hành tin cậy có thể ngoài ra còn bao gồm môđun khởi động hệ thống 446, được tạo cấu hình để khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Hơn nữa, như được thể hiện trên Fig.4f, các chức năng cụ thể của 451 đến 456 là giống như các chức năng tương ứng của 441 đến 446 trên Fig.4e, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Trong thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này:

môđun thu thập 455 còn được tạo cấu hình để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng.

Như được thể hiện trên Fig.4f, thiết bị khởi động nhân hệ điều hành tin

cây có thể ngoài ra còn bao gồm:

môđun đo thứ ba 457, được tạo cấu hình để gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

môđun khởi động chương trình ứng dụng 458, được tạo cấu hình để khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

Các bước phương pháp của các phương án được thể hiện trên Fig.2a đến 2d có thể được thực hiện bởi thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.4f.

Thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này của sáng chế khởi động bộ nạp khởi động môđun khởi động bảo vệ; gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không; nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; nếu mã nhân hệ điều hành là được tin cậy, khởi tạo mã nhân để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và nếu bộ nạp khởi động là được tin cậy, khởi động nhân. Theo giải pháp này, độ an toàn khởi động nhân được nâng cao đến một mức nào đó.

Fig.5a là sơ đồ cấu trúc của phương án khác nữa của thiết bị khởi động nhân hệ điều hành tin cậy theo sáng chế. Thiết bị có thể được gắn hệ thống khởi động hoặc môđun chức năng cố định được thêm mới vào hệ thống, ví dụ như, môđun nền thành phần mềm được tin cậy được thể hiện trên Fig.1. Thiết bị khởi động nhân hệ điều hành tin cậy có thể thực hiện phương pháp khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.3a. Như được thể hiện trên Fig.5a, thiết bị khởi động nhân hệ điều hành tin cậy cụ thể bao gồm: bộ bắt đầu quá trình khởi động 501, bộ đo thứ nhất 502, và bộ khởi động nhân 503, trong đó

bộ bắt đầu quá trình khởi động 501 được tạo cấu hình để khởi động

bộ nạp khởi động môđun khởi động bảo vệ;

môđun đo thứ nhất 502 được tạo cấu hình để gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không, trong đó

môđun đo thứ nhất 502 còn được tạo cấu hình để gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; và

bộ khởi động nhân 503 được tạo cấu hình để: nếu mã nhân hệ điều hành là được tin cậy, chạy mã nhân hệ điều hành để khởi động nhân.

Hơn nữa, như được thể hiện trên Fig.5b, các chức năng cụ thể của 511 đến 513 là giống với các chức năng tương ứng của 501 đến 503 trên Fig.5a, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này có thể ngoài ra còn bao gồm bộ phận thu thập 514, trong đó bộ phận thu thập 514 được tạo cấu hình để:

thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV; và thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR.

Các bước phương pháp của phương án được thể hiện trên Fig.3b có thể được thực hiện bởi thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.5b.

Hơn nữa, như được thể hiện trên Fig.5c, các chức năng cụ thể của 521 đến 523 là giống với các chức năng tương ứng của 501 đến 503 trên Fig.5a, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này có thể ngoài ra còn bao gồm:

bộ đo thứ hai 525, được tạo cấu hình để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không, trong đó

bộ đo thứ hai 525 còn được tạo cấu hình để: nếu bộ nạp khởi động là được tin cậy, gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

bộ khởi động hệ thống 526, được tạo cấu hình để khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Các bước phương pháp của phương án được thể hiện trên Fig.3c có thể được thực hiện bởi thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.5c.

Hơn nữa, như được thể hiện trên Fig.5d, các chức năng cụ thể của 531 đến 533, 535 và 536 là giống với các chức năng tương ứng của 521 đến 523, 525 và 526 trên Fig.5c, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này có thể ngoài ra còn bao gồm:

bộ đo thứ ba 537, được tạo cấu hình để gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

bộ phận khởi động chương trình ứng dụng 538, được tạo cấu hình để khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

Các bước phương pháp của phương án được thể hiện trên Fig.3d có thể được thực hiện bởi thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.5d.

Hơn nữa, như được thể hiện trên Fig.5e, các chức năng cụ thể của 541 đến 544 là giống với các chức năng tương ứng của 511 đến 514 trên Fig.5b, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này có thể ngoài ra còn bao gồm:

bộ đo thứ hai 545, được tạo cấu hình để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không, trong đó

bộ đo thứ hai 545 còn được tạo cấu hình để: nếu bộ nạp khởi động là

được tin cậy, gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

bộ khởi động hệ thống 546, được tạo cấu hình để khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

Trong thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.5e, bộ phận thu thập 544 còn được tạo cấu hình để: thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR.

Hơn nữa, như được thể hiện trên Fig.5f, các chức năng cụ thể của 551 đến 556 là giống tương ứng với các chức năng của 541 đến 546 trên Fig.5e, và các chi tiết sẽ không được mô tả sau đây một lần nữa. Trong thiết bị khởi động nhân hệ điều hành tin cậy được cung cấp trong phương án này:

bộ phận thu thập 554 còn được tạo cấu hình để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng.

Như được thể hiện trên Fig.5f, thiết bị khởi động nhân hệ điều hành tin cậy có thể ngoài ra còn bao gồm:

môđun đo thứ ba 557, được tạo cấu hình để gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

môđun khởi động chương trình ứng dụng 558, được tạo cấu hình để khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

Các bước phương pháp của các phương án được thể hiện trên Fig.3a đến 3d có thể được thực hiện bởi thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trên Fig.5f.

Thiết bị khởi động nhân hệ điều hành tin cậy được thể hiện trong phương án này khởi động bộ nạp khởi động môđun khởi động bảo vệ; gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không; nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi

động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; nếu mã nhân hệ điều hành là được tin cậy, chạy mã nhân hệ điều hành để khởi động nhân. So sánh với phương án được thể hiện trên Fig.4a, rằng nhân đo bộ nạp khởi động một lần nữa trong quy trình khởi động được loại bỏ, và toàn bộ nhân được khởi động trực tiếp, khiến đơn giản hóa thủ tục khởi động nhân đến một mức nào đó. Độ an toàn khi nhân được khởi động cũng được nâng cao bằng cách đo độ an toàn của phân khu PCR trước khi nhân được tải.

Người có trình độ trung bình trong lĩnh vực hiển nhiên có thể hiểu rằng, nhằm mục đích thuận tiện và mô tả ngắn gọn, việc phân chia các mô đun chức năng nêu trên được lấy làm ví dụ để minh họa. Trong ứng dụng thực tế, các chức năng nêu trên có thể được đặt trong các mô đun chức năng khác nhau và được thực hiện theo yêu cầu, nghĩa là, cấu trúc bên trong của thiết bị được chia thành các mô đun chức năng khác nhau để thực hiện toàn bộ hoặc một số các chức năng được mô tả ở trên. Đối với quy trình hoạt động cụ thể của hệ thống, thiết bị và bộ phận nêu trên, tham chiếu có thể được thực hiện với quy trình xử lý tương tự trong các phương án phương án nêu trên, và các chi tiết sẽ không được mô tả sau đây một lần nữa.

Trong một số phương án được đề xuất theo sáng chế, cần phải hiểu rằng hệ thống, thiết bị và phương pháp được bộc lộ có thể được thực hiện theo các cách khác nhau. Ví dụ như, phương án thiết bị được mô tả được mô tả chỉ đơn thuần là minh họa. Ví dụ như, việc phân chia mô đun hoặc bộ phận chỉ đơn thuần là việc phân chia chức năng một cách logic và có thể có cách phân chia khác trong cách thực hiện thực tế. Ví dụ như, nhiều bộ phận hoặc thành phần có thể được kết hợp hoặc được tích hợp vào một hệ thống khác, hoặc một số đặc điểm có thể bị bỏ qua hoặc không được thực hiện. Ngoài ra, các ghép nối tương đồng được hiển thị hoặc được thảo luận hoặc các ghép nối trực tiếp hoặc các kết nối truyền thông có thể được thực hiện bằng cách sử dụng một số giao diện. Việc ghép nối không trực tiếp hoặc kết nối truyền thông giữa các thiết bị hoặc các bộ

phần có thể được thực hiện dưới dạng điện tử, cơ khí hoặc các dạng khác.

Các bộ phận được mô tả làm các phần riêng biệt có thể hoặc có thể không tách biệt một cách vật lý, và các phần được thể hiện là các bộ phận có thể hoặc có thể không phải là các bộ phận theo cách vật lý, có thể được đặt tại cùng một vị trí, hoặc có thể được phân bố trên nhiều bộ phận mạng. Một số hoặc toàn bộ các bộ phận có thể được lựa chọn theo nhu cầu thực tế để đạt được các mục đích của các giải pháp của các phương án.

Ngoài ra, các bộ phận chức năng trong các phương án của sáng chế có thể được tích hợp thành một bộ phận xử lý, hoặc mỗi bộ phận có thể tồn tại riêng về mặt vật lý, hoặc hai bộ phận hoặc nhiều hơn được tích hợp thành một bộ phận. Bộ phận tích hợp có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng bộ phận chức năng phần mềm.

Khi bộ phận tích hợp nêu trên được thực hiện dưới dạng bộ phận chức năng phần mềm và được bán hoặc được sử dụng như một sản phẩm độc lập, bộ phận tích hợp có thể được lưu trữ trong phương tiện lưu trữ đọc được bởi máy tính. Dựa vào hiểu biết như vậy, các giải pháp kỹ thuật của sáng chế về cơ bản, hoặc một phần đóng góp vào kỹ thuật đã biết, hoặc toàn bộ hoặc một phần các giải pháp kỹ thuật có thể được thực hiện dưới dạng sản phẩm phần mềm. Sản phẩm phần mềm được lưu trữ trong phương tiện lưu trữ và bao gồm một số chỉ dẫn để chỉ dẫn thiết bị máy tính (mà có thể là máy tính cá nhân, máy chủ, hoặc thiết bị mạng) hoặc bộ xử lý để thực hiện tất cả hoặc một phần các bước của phương pháp được mô tả trong các phương án của sáng chế. Phương tiện lưu trữ nêu trên bao gồm: phương tiện bất kỳ mà có thể lưu trữ mã chương trình, chẳng hạn như ổ đĩa chớp USB, đĩa cứng tháo lắp được, bộ nhớ chỉ đọc (ROM, Read-Only Memory), bộ nhớ truy cập ngẫu nhiên (RAM, Random Access Memory), đĩa từ, hoặc đĩa quang.

Các phương án được mô tả ở trên chỉ đơn thuần nhằm mục đích mô tả các giải pháp kỹ thuật của sáng chế, chứ không nhằm để giới hạn sáng chế. Mặc dù sáng chế được mô tả chi tiết dựa vào các phương án nêu trên, người có trình độ trung bình trong lĩnh vực kỹ thuật tương ứng cần hiểu rằng họ vẫn có thể

thực hiện các cải biến đối với các giải pháp kỹ thuật được mô tả trong các phương án nêu trên hoặc thực hiện các thay thế tương đương đối với một số đặc điểm kỹ thuật của nó, mà không trệch khỏi phạm vi của các giải pháp kỹ thuật của các phương án của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp khởi động nhân hệ điều hành tin cậy bao gồm các bước:

khởi động bộ nạp khởi động môđun khởi động bảo vệ;

gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không;

gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân hệ điều hành vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không;

khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân hệ điều hành để kích hoạt nhân hệ điều hành được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và

khởi động nhân hệ điều hành nếu bộ nạp khởi động là được tin cậy.

2. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 1, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV; và

việc gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không bao gồm các bước:

gọi bộ nạp khởi động để tính giá trị đo thực phân khu PCR theo thuật toán bảo vệ thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực phân khu PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có được tin cậy hay không, trong đó nếu giá trị đo thực phân khu PCR bằng giá trị đo chuẩn phân khu PCR, phân khu PCR là được tin cậy.

3. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 2, trong đó việc thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV bao gồm các bước:

tạo ra khóa gốc dựa vào PIN được đưa vào bởi người dùng; và

giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá trị đo

chuẩn phân khu PCR được lưu trữ trước trong phân khu ENC.

4. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR; và

việc gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân hệ điều hành vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không bao gồm các bước:

nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân hệ điều hành vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân hệ điều hành theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã nhân hệ điều hành có bằng giá trị đo mã nhân hệ điều hành chuẩn hay không, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân hệ điều hành bằng giá trị đo mã nhân hệ điều hành chuẩn, mã nhân hệ điều hành là được tin cậy.

5. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và

việc khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân hệ điều hành để kích hoạt nhân hệ điều hành được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không bao gồm các bước:

nếu mã nhân hệ điều hành là được tin cậy, khởi tạo mã nhân hệ điều hành để kích hoạt nhân hệ điều hành được khởi tạo để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn bộ nạp khởi động hay không, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực

bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, bộ nạp khởi động là được tin cậy.

6. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 1 đến 5, sau việc khởi động nhân, trong đó còn bao gồm các bước:

gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

7. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 6, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

việc gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không bao gồm các bước:

gọi nhân để tính giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân hay không, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

8. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 6 hoặc 7, sau việc khởi động hệ điều hành, trong đó còn bao gồm các bước:

gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

9. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 8, trong đó

phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng; và

việc gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không bao gồm các bước:

gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn của chương trình ứng dụng hay không, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, chương trình ứng dụng là được tin cậy.

10. Phương pháp khởi động nhân hệ điều hành tin cậy bao gồm các bước:

khởi động bộ nạp khởi động môđun khởi động bảo vệ;

gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không;

gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; và

nếu mã nhân hệ điều hành là được tin cậy, chạy mã nhân hệ điều hành để khởi động nhân.

11. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 10, sau việc chạy mã nhân hệ điều hành để khởi động nhân, trong đó còn bao gồm các bước:

gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không;

nếu bộ nạp khởi động là được tin cậy, gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là

được tin cậy.

12. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 10 hoặc 11, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV; và

việc gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không bao gồm các bước:

gọi bộ nạp khởi động để tính giá trị đo thực phân khu PCR theo thuật toán bảo vệ thứ nhất được lưu trữ trước, và đo, bằng cách so sánh xem giá trị đo thực phân khu PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có được tin cậy hay không, trong đó nếu giá trị đo thực phân khu PCR bằng giá trị đo chuẩn phân khu PCR, phân khu PCR là được tin cậy.

13. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 12, trong đó việc thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV bao gồm các bước:

tạo ra khóa gốc dựa vào PIN được đưa vào bởi người dùng; và

giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu ENV, của phân khu PCR.

14. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 10 đến 13, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR; và

việc gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không bao gồm các bước:

nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã

nhân có bằng giá trị đo mã nhân hệ điều hành chuẩn hay không, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân bằng giá trị đo mã nhân hệ điều hành chuẩn, mã nhân hệ điều hành là được tin cậy.

15. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 11 đến 14, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và

việc gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không bao gồm các bước:

gọi nhân để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn bộ nạp khởi động hay không, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, bộ nạp khởi động là được tin cậy.

16. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 11 đến 15, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

việc gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không bao gồm các bước:

gọi nhân để tính giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân hay không, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

17. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 11 đến 16, sau việc khởi động hệ điều hành, trong đó còn

bao gồm các bước:

gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

18. Phương pháp khởi động nhân hệ điều hành tin cậy theo điểm 17, trong đó phương pháp còn bao gồm các bước:

thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng; và

việc gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không bao gồm các bước:

gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn của chương trình ứng dụng hay không, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, chương trình ứng dụng là được tin cậy.

19. Thiết bị khởi động nhân hệ điều hành tin cậy bao gồm:

môđun bắt đầu quá trình khởi động, được tạo cấu hình để khởi động bộ nạp khởi động môđun khởi động bảo vệ;

môđun đo thứ nhất, được tạo cấu hình để gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không, trong đó:

môđun đo thứ nhất còn được tạo cấu hình để gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không;

môđun đo thứ hai, được tạo cấu hình để khởi tạo, nếu mã nhân hệ điều hành là được tin cậy, mã nhân để kích hoạt nhân được khởi tạo để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không; và

môđun khởi động nhân, được tạo cấu hình để khởi động nhân nếu bộ nạp khởi động là được tin cậy.

20. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 19, trong đó thiết bị còn bao gồm:

môđun thu thập, được tạo cấu hình để thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV, trong đó:

môđun đo thứ nhất được tạo cấu hình một cách đặc biệt để gọi bộ nạp khởi động để tính giá trị đo thực phân khu PCR theo thuật toán bảo vệ thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực phân khu PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có được tin cậy hay không, trong đó nếu giá trị đo thực phân khu PCR bằng giá trị đo chuẩn phân khu PCR, xác định được rằng phân khu PCR là được tin cậy.

21. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 20, trong đó:

môđun thu thập được tạo cấu hình một cách đặc biệt để tạo ra khóa gốc dựa vào PIN được đưa vào bởi người dùng, và giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu ENV, của phân khu PCR.

22. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 19 đến 21, trong đó:

môđun thu thập còn được tạo cấu hình để thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR; và

môđun đo thứ nhất được tạo cấu hình một cách đặc biệt để: nếu phân khu PCR là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã nhân có bằng giá trị đo mã nhân hệ điều hành chuẩn hay không, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân bằng giá trị đo mã nhân hệ điều

hành chuẩn, mã nhân hệ điều hành là được tin cậy.

23. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 19 đến 22, trong đó:

môđun thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và

môđun đo thứ hai được tạo cấu hình một cách đặc biệt để: nếu mã nhân hệ điều hành là được tin cậy, khởi tạo mã nhân để kích hoạt nhân được khởi tạo để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn bộ nạp khởi động hay không, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, bộ nạp khởi động là được tin cậy.

24. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 19 đến 23, trong đó thiết bị còn bao gồm môđun khởi động hệ thống, trong đó:

môđun đo thứ hai còn được tạo cấu hình để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

môđun khởi động hệ thống được tạo cấu hình để khởi động hệ điều hành nếu môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

25. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 24, trong đó:

môđun thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

môđun đo thứ hai được tạo cấu hình một cách đặc biệt để gọi nhân để tính giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân hay không, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, môđun

nâng cao việc quản lý bảo vệ nhân là được tin cậy.

26. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 24 hoặc 25, trong đó thiết bị còn bao gồm:

môđun đo thứ ba, được tạo cấu hình để gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

môđun khởi động chương trình ứng dụng, được tạo cấu hình để khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

27. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 26, trong đó:

môđun thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng; và

môđun đo thứ ba được tạo cấu hình một cách đặc biệt để gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn của chương trình ứng dụng hay không, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, chương trình ứng dụng là được tin cậy.

28. Thiết bị khởi động nhân hệ điều hành tin cậy bao gồm:

bộ bắt đầu quá trình khởi động, được tạo cấu hình để khởi động bộ nạp khởi động môđun khởi động bảo vệ;

bộ đo thứ nhất, được tạo cấu hình để gọi bộ nạp khởi động để đo, theo thuật toán bảo vệ thứ nhất, xem phân khu thanh ghi cấu hình nền (PCR) có được tin cậy hay không, trong đó:

bộ đo thứ nhất còn được tạo cấu hình để gọi, nếu phân khu PCR là được tin cậy, bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, và gọi bộ nạp khởi động để đo, theo thuật toán kết thúc thứ nhất và giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR, xem mã nhân hệ điều hành có được tin cậy hay không; và

bộ khởi động nhân, được tạo cấu hình để: nếu mã nhân hệ điều hành là

được tin cậy, chạy mã nhân hệ điều hành để khởi động nhân.

29. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 28, trong đó thiết bị còn bao gồm:

bộ đo thứ hai, được tạo cấu hình để gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ hai, xem bộ nạp khởi động có được tin cậy hay không, trong đó:

bộ đo thứ hai còn được tạo cấu hình để: nếu bộ nạp khởi động là được tin cậy, gọi nhân hệ điều hành để đo, theo thuật toán kết thúc thứ ba, xem mô đun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không; và

bộ khởi động hệ thống, được tạo cấu hình để khởi động hệ điều hành nếu mô đun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

30. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 28 hoặc 29, trong đó thiết bị còn bao gồm:

bộ phận thu thập, được tạo cấu hình để thu thập giá trị đo chuẩn phân khu PCR được lưu trữ trước trong phân khu môi trường ENV, trong đó:

bộ đo thứ nhất được tạo cấu hình một cách đặc biệt để gọi bộ nạp khởi động để tính giá trị đo thực phân khu PCR theo thuật toán bảo vệ thứ nhất được lưu trữ trước, và đo, bằng cách so sánh xem giá trị đo thực phân khu PCR có bằng giá trị đo chuẩn phân khu PCR hay không, xem phân khu PCR có được tin cậy hay không, trong đó nếu giá trị đo thực phân khu PCR bằng giá trị đo chuẩn phân khu PCR, phân khu PCR là được tin cậy.

31. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 30, trong đó:

bộ phận thu thập được tạo cấu hình một cách đặc biệt để tạo ra khóa gốc dựa vào PIN được đưa vào bởi người dùng, và giải mã phân khu ENV bằng cách sử dụng khóa gốc, để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu ENV, của phân khu PCR.

32. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 28 đến 31, trong đó:

bộ phận thu thập còn được tạo cấu hình để thu thập giá trị đo mã nhân hệ điều hành chuẩn được lưu trữ trước trong phân khu PCR; và

bộ đo thứ nhất được tạo cấu hình một cách đặc biệt để: nếu phân khu PCR

là được tin cậy, gọi bộ nạp khởi động để đọc mã nhân vào trong bộ nhớ, gọi bộ nạp khởi động để tính giá trị đo thực mã nhân theo thuật toán kết thúc thứ nhất, và đo, bằng cách so sánh xem giá trị đo thực mã nhân có bằng giá trị đo mã nhân hệ điều hành chuẩn hay không, xem mã nhân hệ điều hành có được tin cậy hay không, trong đó nếu giá trị đo thực mã nhân bằng giá trị đo mã nhân hệ điều hành chuẩn, mã nhân hệ điều hành là được tin cậy.

33. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 29 đến 32, trong đó:

bộ phận thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn bộ nạp khởi động được lưu trữ trước trong phân khu PCR; và

bộ đo thứ hai được tạo cấu hình một cách đặc biệt để gọi nhân để tính giá trị đo thực bộ nạp khởi động theo thuật toán kết thúc thứ hai, và đo, bằng cách so sánh xem giá trị đo thực bộ nạp khởi động có bằng giá trị đo chuẩn bộ nạp khởi động hay không, xem bộ nạp khởi động có được tin cậy hay không, trong đó nếu giá trị đo thực bộ nạp khởi động bằng giá trị đo chuẩn bộ nạp khởi động, bộ nạp khởi động là được tin cậy.

34. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 29 đến 33, trong đó:

bộ phận thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân được lưu trữ trước trong phân khu PCR; và

bộ đo thứ hai được tạo cấu hình một cách đặc biệt để gọi nhân để tính giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân theo thuật toán kết thúc thứ ba, và đo, bằng cách so sánh xem giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân có bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân hay không, xem môđun nâng cao việc quản lý bảo vệ nhân có được tin cậy hay không, trong đó nếu giá trị đo thực môđun nâng cao việc quản lý bảo vệ nhân bằng giá trị đo chuẩn môđun nâng cao việc quản lý bảo vệ nhân, môđun nâng cao việc quản lý bảo vệ nhân là được tin cậy.

35. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm bất kỳ trong số các điểm từ 29 đến 34, trong đó thiết bị còn bao gồm:

bộ đo thứ ba, được tạo cấu hình để gọi môđun nâng cao việc quản lý bảo vệ nhân hệ điều hành để đo, theo thuật toán kết thúc thứ tư, xem chương trình ứng dụng cần được khởi động có được tin cậy hay không; và

bộ phận khởi động chương trình ứng dụng, được tạo cấu hình để khởi động chương trình ứng dụng nếu chương trình ứng dụng là được tin cậy.

36. Thiết bị khởi động nhân hệ điều hành tin cậy theo điểm 35, trong đó:

bộ phận thu thập còn được tạo cấu hình để thu thập giá trị đo chuẩn, mà được lưu trữ trước trong phân khu PCR, của chương trình ứng dụng; và

bộ đo thứ ba được tạo cấu hình một cách đặc biệt để gọi môđun nâng cao việc quản lý bảo vệ nhân để tính giá trị đo thực của chương trình ứng dụng theo thuật toán kết thúc thứ tư, và đo, bằng cách so sánh xem giá trị đo thực của chương trình ứng dụng có bằng giá trị đo chuẩn của chương trình ứng dụng hay không, xem chương trình ứng dụng có được tin cậy hay không, trong đó nếu giá trị đo thực của chương trình ứng dụng bằng giá trị đo chuẩn của chương trình ứng dụng, chương trình ứng dụng là được tin cậy.

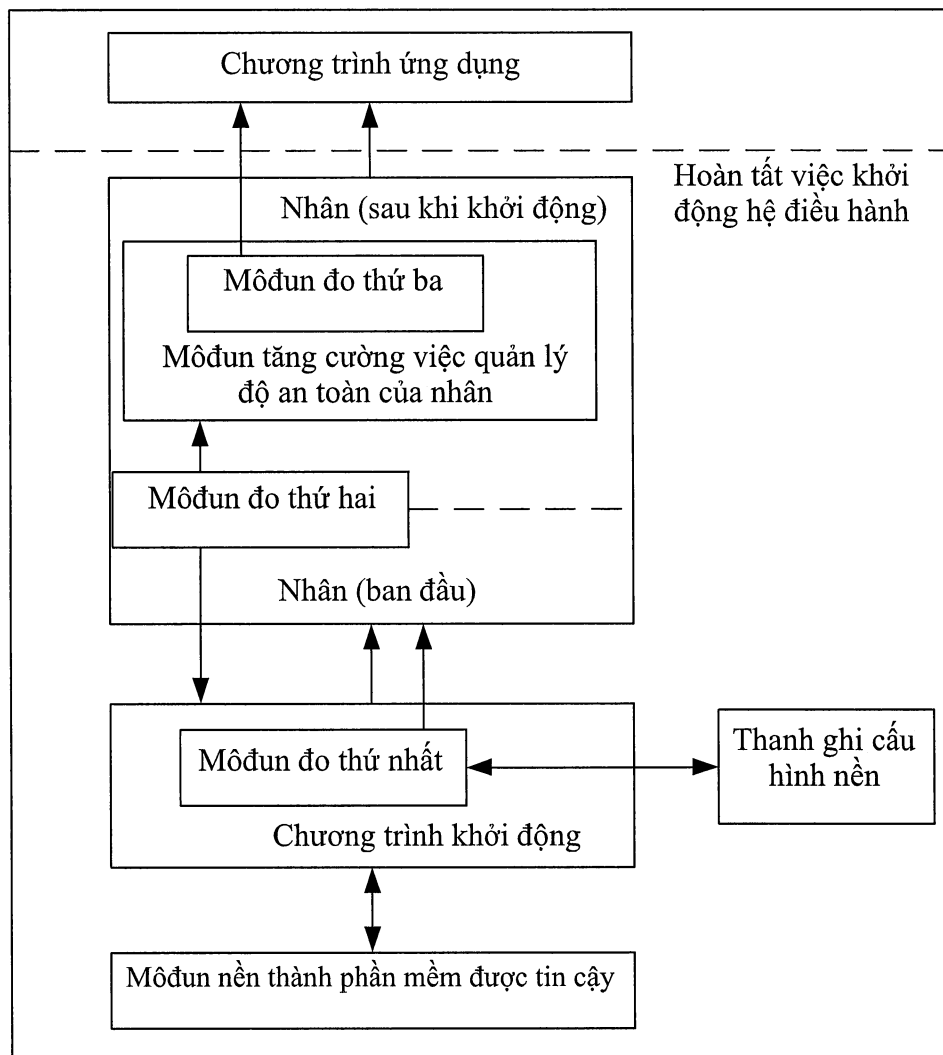


FIG. 1

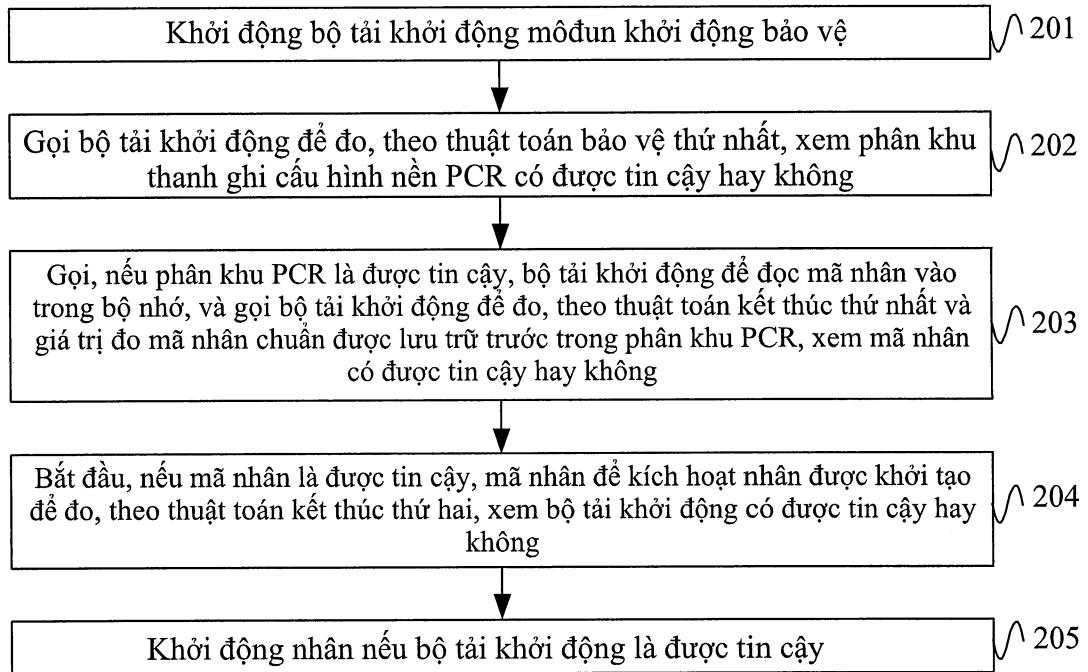


FIG. 2a

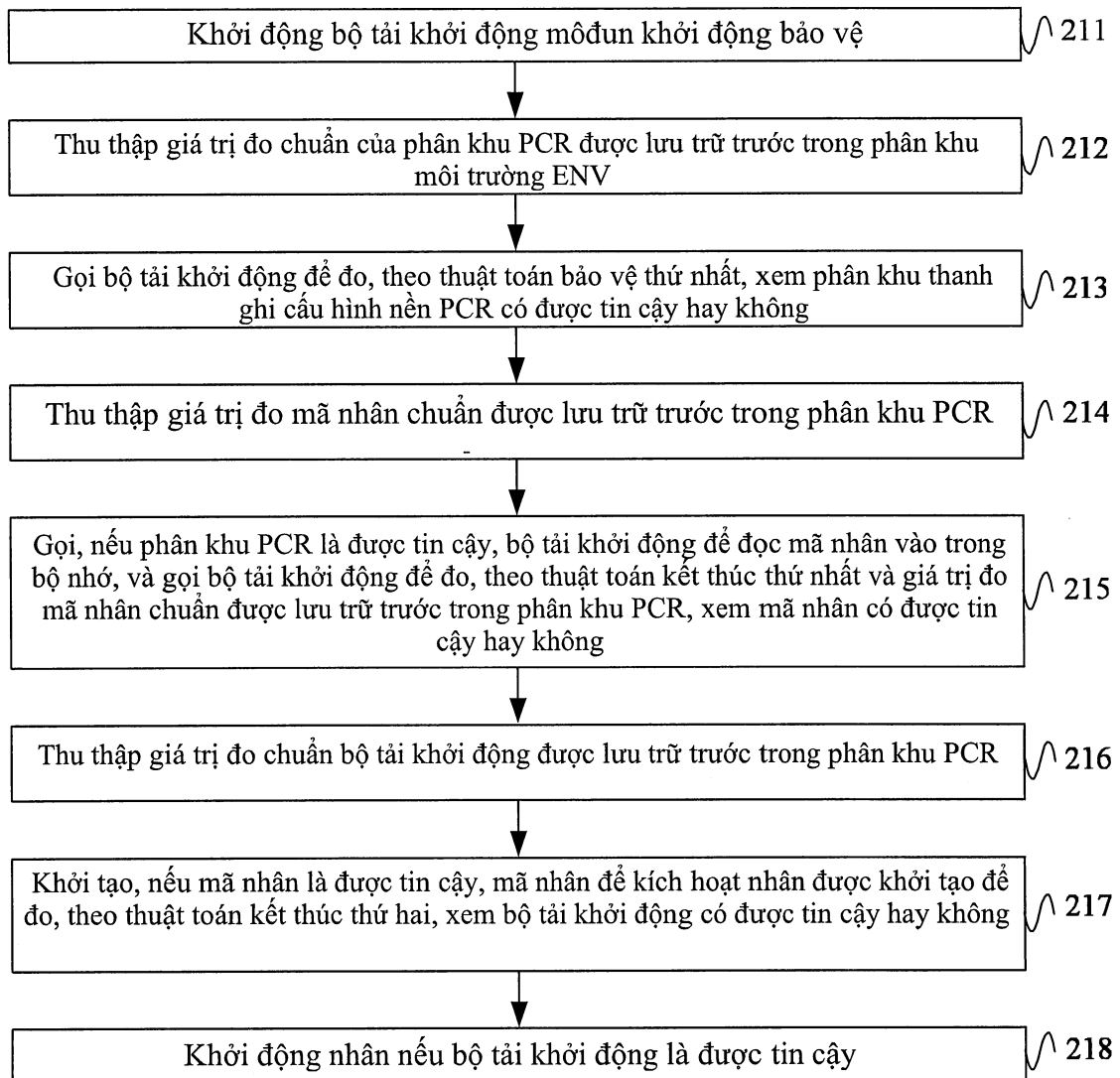


FIG. 2b

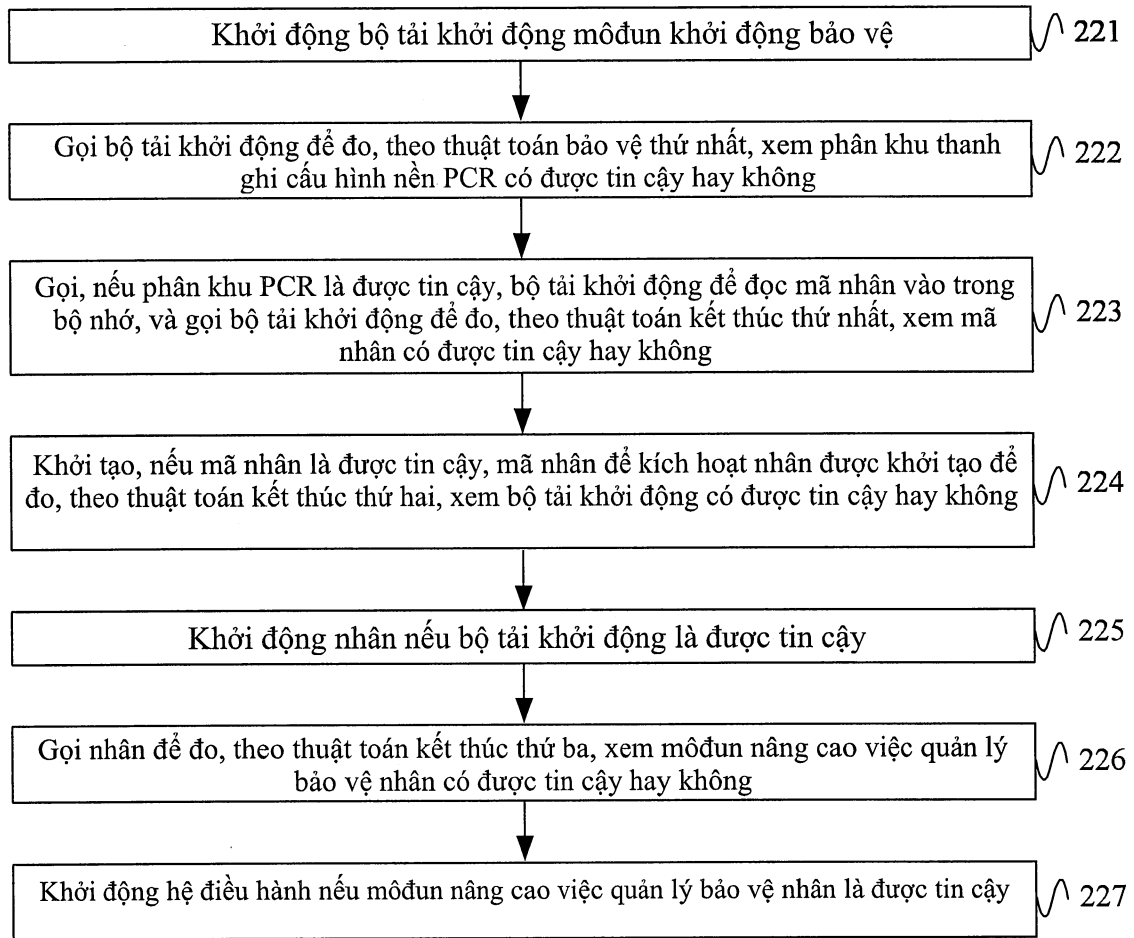


FIG. 2c

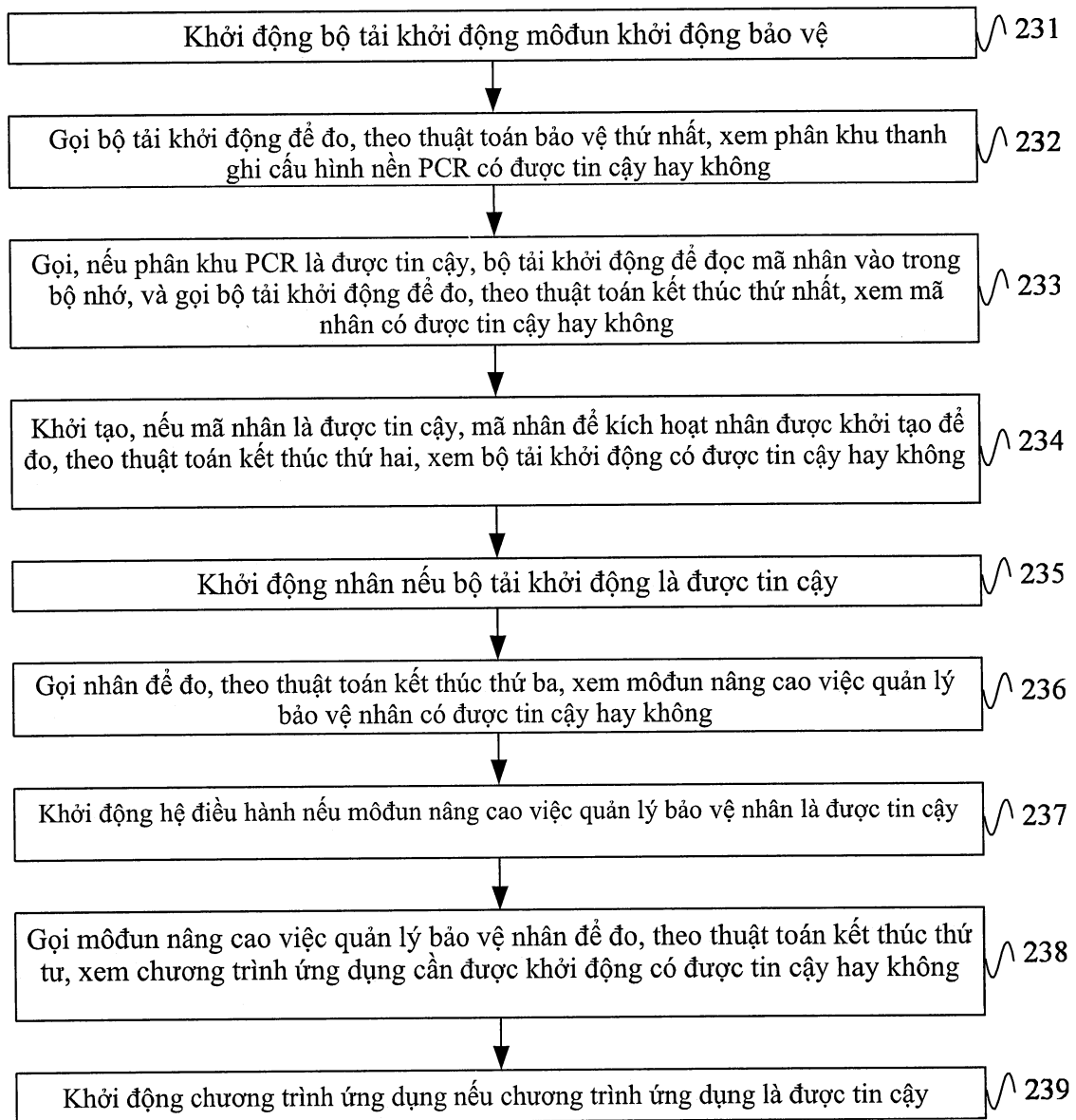
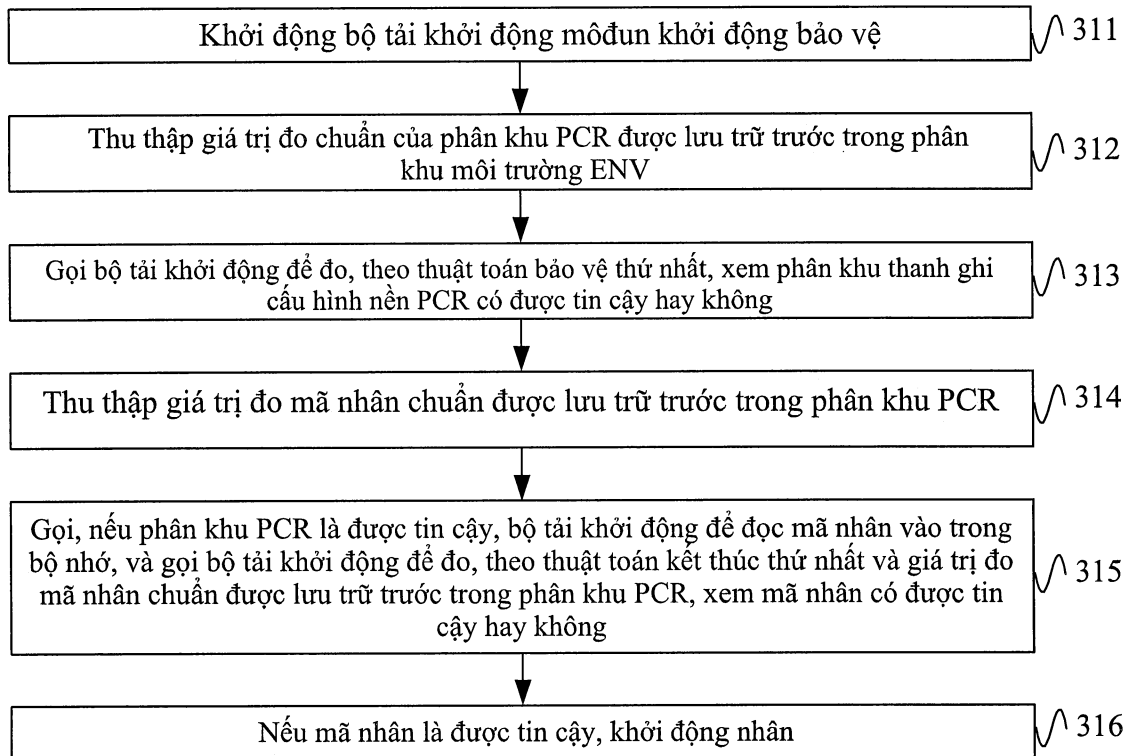
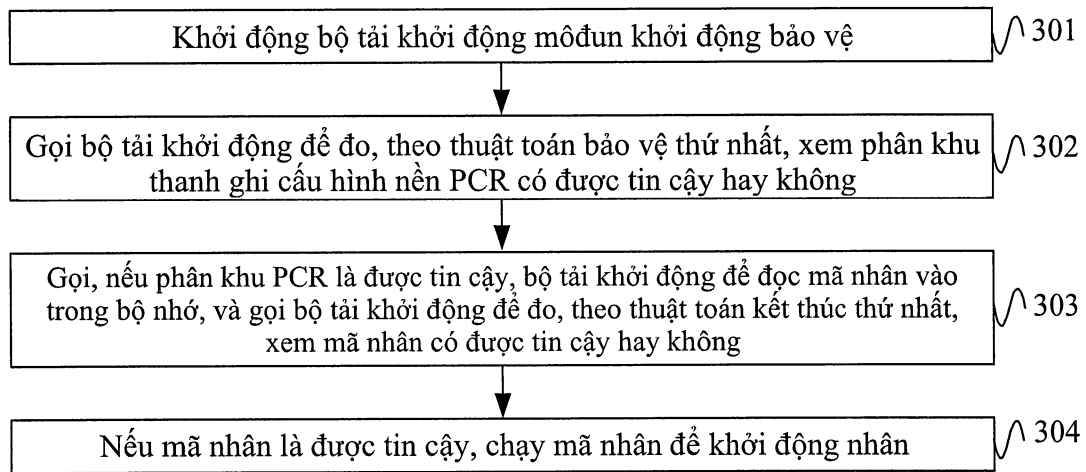


FIG. 2d



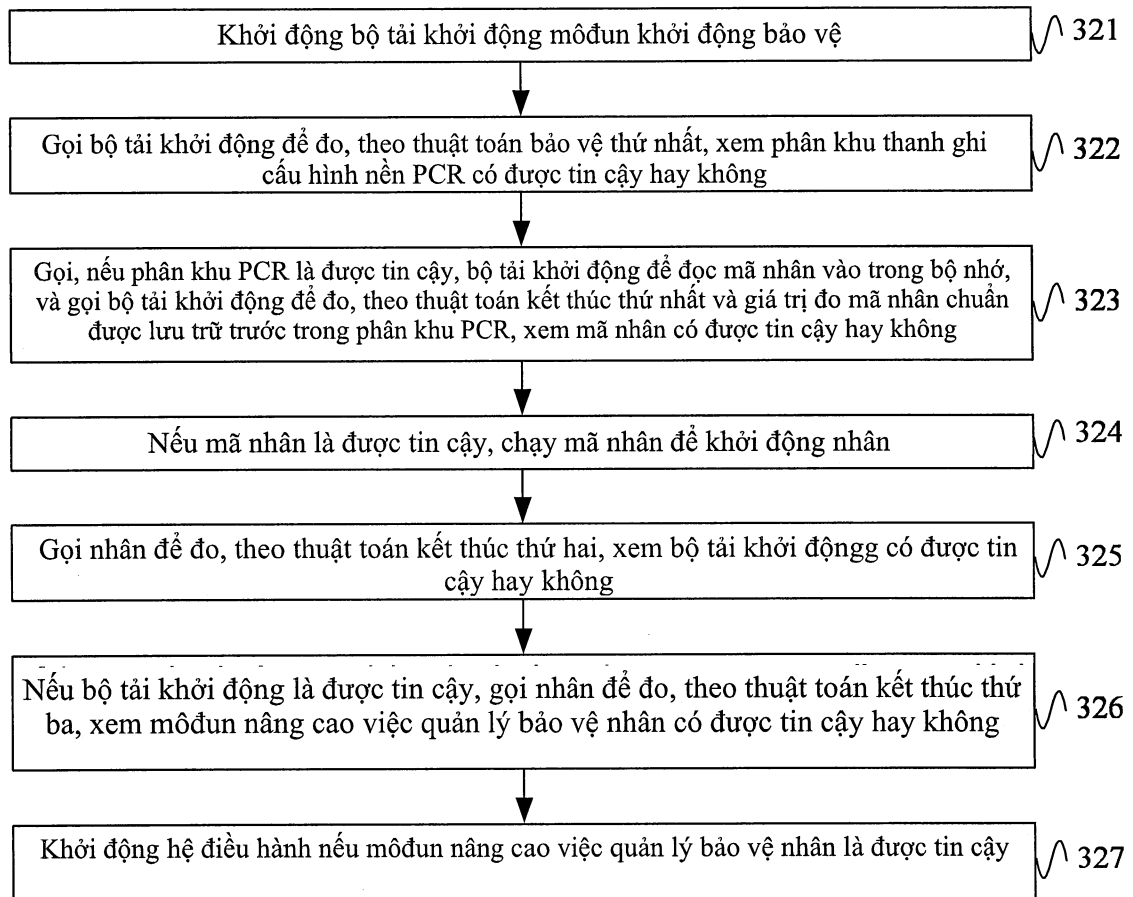


FIG. 3c

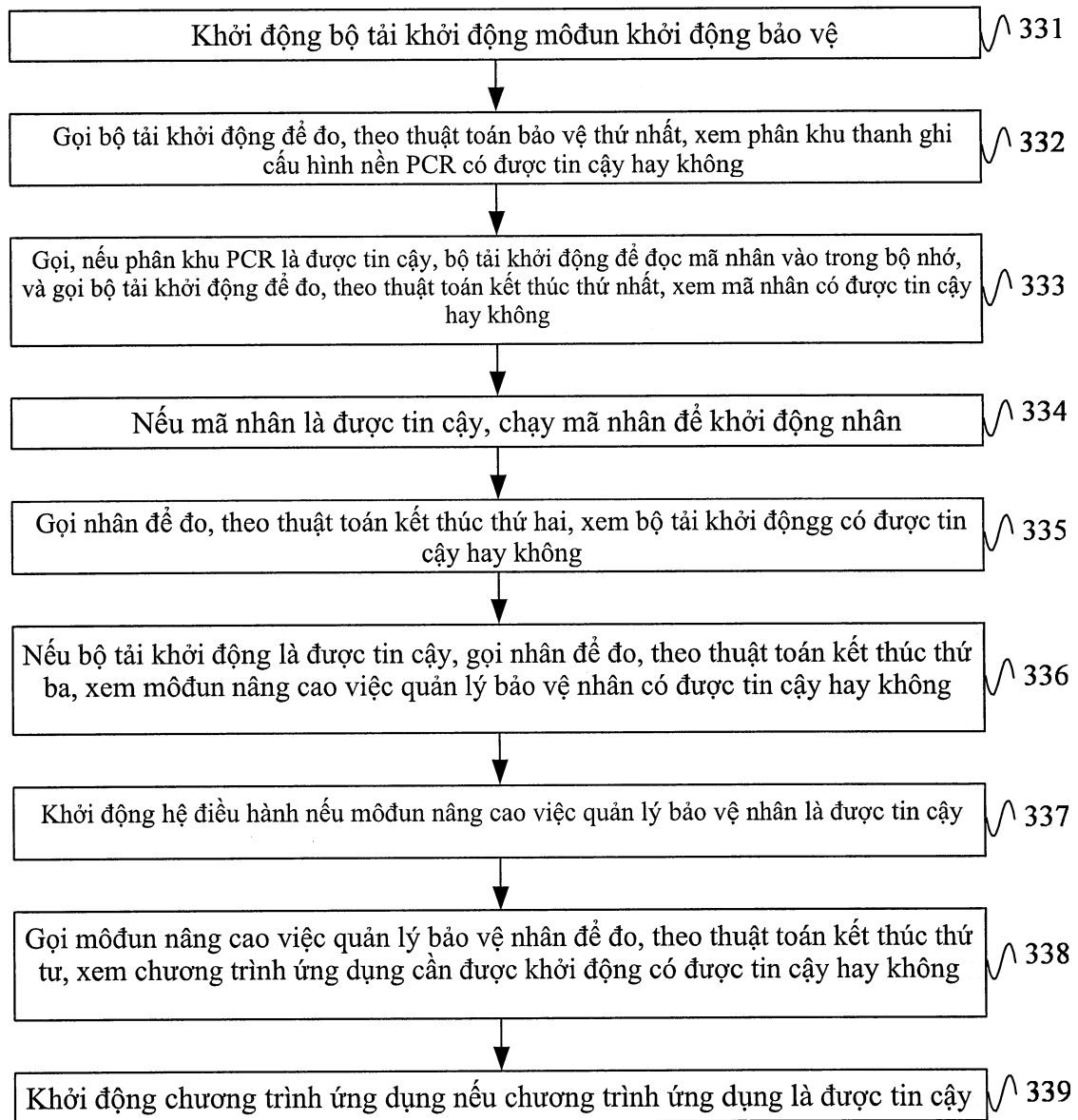


FIG. 3d

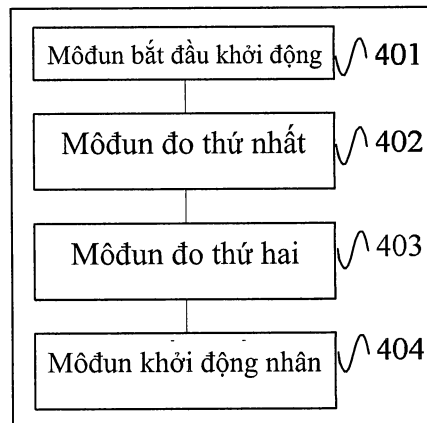


FIG. 4a

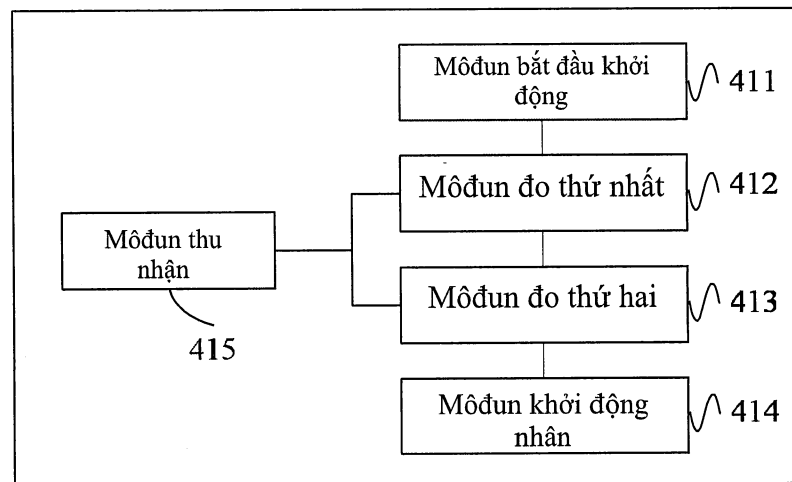


FIG. 4b

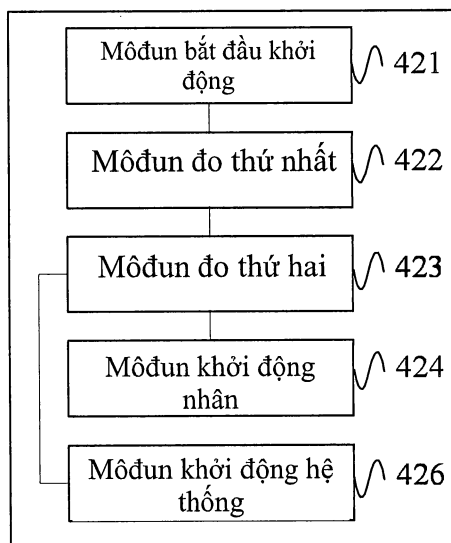


FIG. 4c

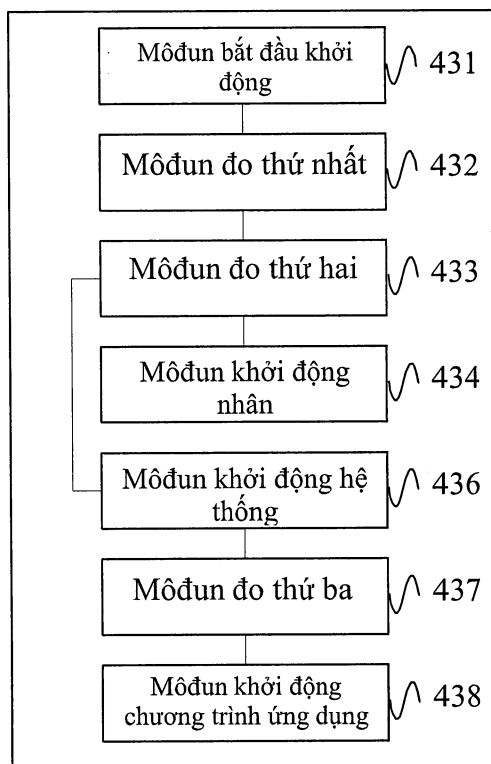


FIG. 4d

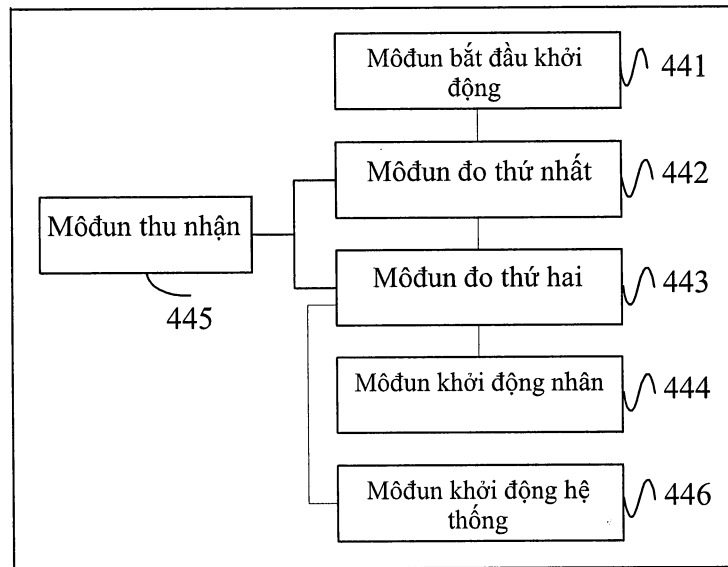


FIG. 4e

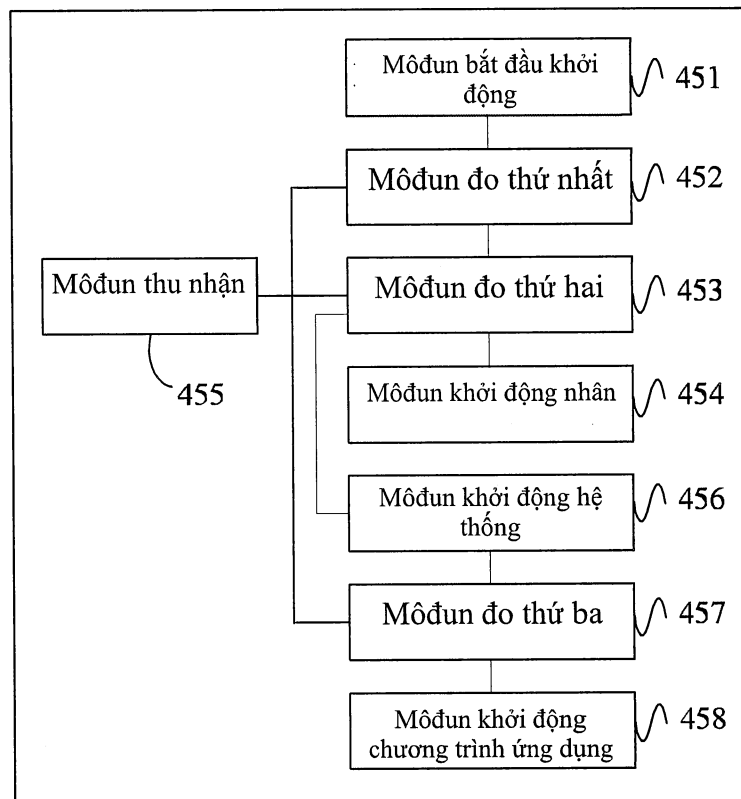


FIG. 4f

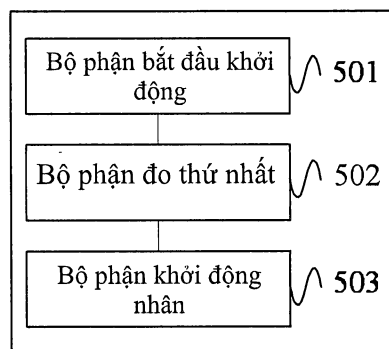


FIG. 5a

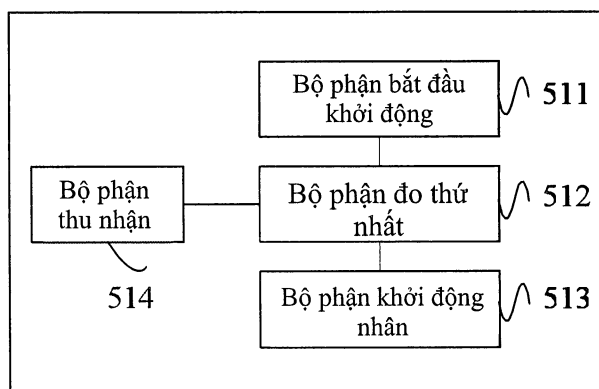


FIG. 5b

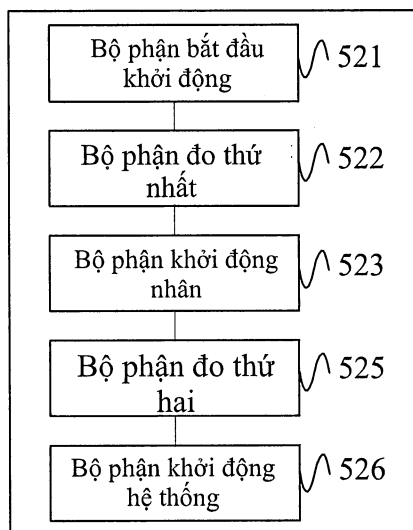


FIG. 5c

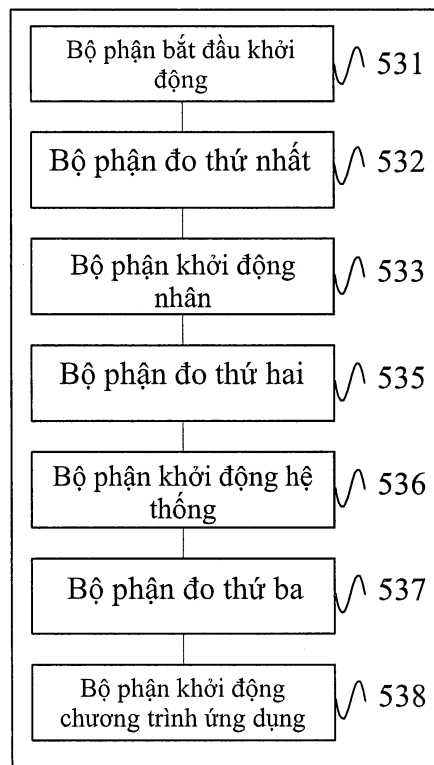


FIG. 5d

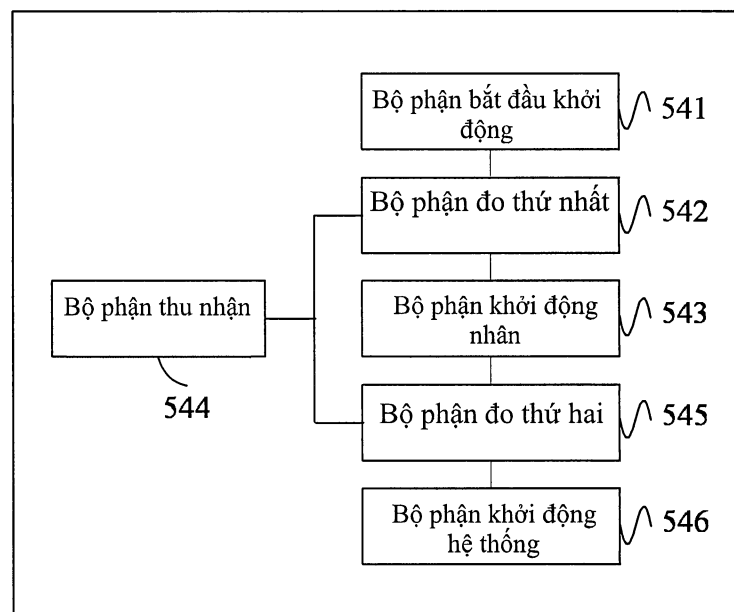


FIG. 5e

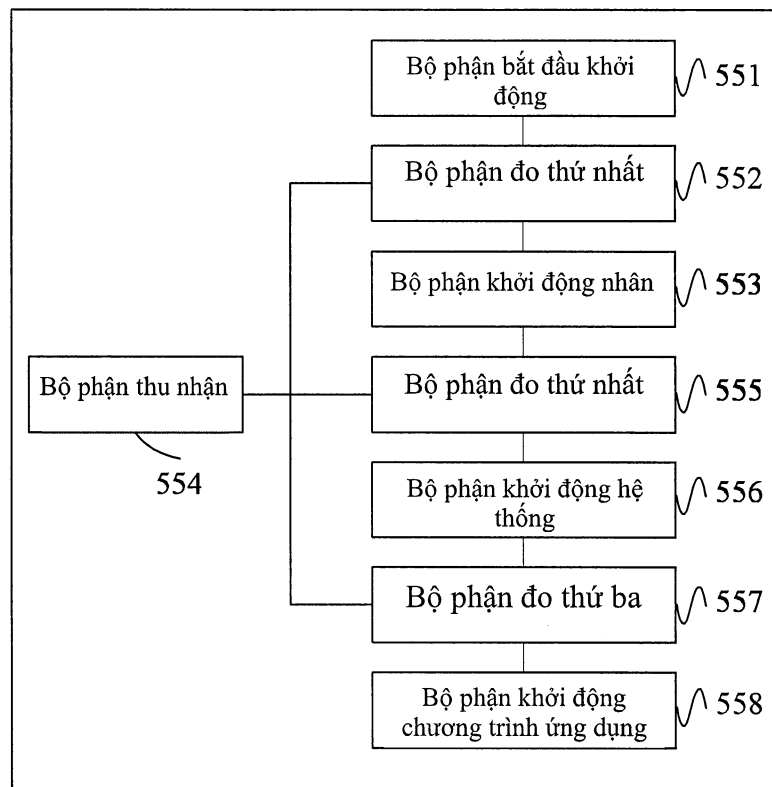


FIG. 5f