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

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

(11) **1-0053194**

(51)[2022.01] **G06F 21/79**

(13) **B**

(21) 1-2023-00285
(22) 19/07/2021
(86) PCT/US2021/042148 19/07/2021
(87) WO 2022/020225 A1 27/01/2022
(30) 16/937,907 24/07/2020 US
(45) 25/11/2025 452
(43) 25/05/2023 422A
(73) QUALCOMM INCORPORATED (US)
ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, CA 92121-1714, United States of America
(72) LI, Yanru (US); CHUN, Dexter Tamio (US).
(74) Công ty TNHH Quốc tế D &N (D&N INTERNATIONAL CO.,LTD.)

(54) PHƯƠNG PHÁP CHỈ BÁO PHẢN HỒI VỀ VIỆC CHẤP NHẬN TRUY CẬP/VI PHẠM CHO HỆ THỐNG TRÊN CHIP VÀ THIẾT BỊ NHỚ

(21) 1-2023-00285

(57) Sáng chế đề cập đến phương pháp chỉ báo phản hồi về việc chấp nhận truy cập/vi phạm cho hệ thống trên chip và thiết bị nhớ. Các phương án khác nhau có thể bao gồm các phương pháp và hệ thống để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (system-on-a-chip - SOC). Các phương pháp khác nhau có thể bao gồm bước nhận bản tin cấu hình từ SOC để tạo cấu hình điều khiển truy cập bộ nhớ của thiết bị nhớ và tạo cấu hình điều khiển truy cập bộ nhớ dựa trên bản tin cấu hình. Các phương án khác nhau có thể bao gồm bước nhận bản tin yêu cầu truy cập từ SOC yêu cầu truy cập vào địa chỉ cơ sở của bộ nhớ và phạm vi truy cập bộ nhớ của mảng ô nhớ của thiết bị nhớ, trong đó bản tin yêu cầu truy cập bao gồm hoạt động đọc/ghi. Các phương án khác nhau có thể bao gồm việc so sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ đã được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được cho phép hay không. Các phương án khác nhau có thể còn bao gồm việc thực hiện hoạt động đọc/ghi để đáp lại việc xác định rằng bản tin yêu cầu truy cập được cho phép.

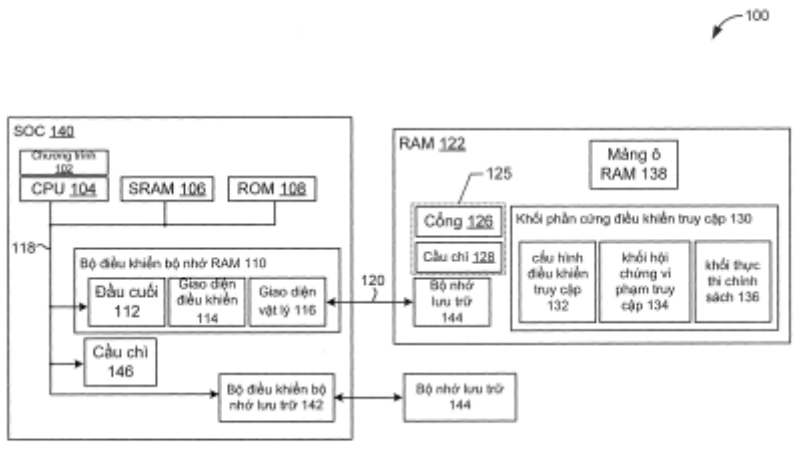

FIG. 1

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến các phương pháp và hệ thống cấp quyền truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (system-on-a-chip - SOC).

Tình trạng kỹ thuật của sáng chế

Thông thường, điều khiển truy cập bộ nhớ hệ thống đã được triển khai như chức năng độc quyền trong bộ xử lý ứng dụng (application processor - AP) hoặc hệ thống trên chip (SOC), bởi phía máy chính chẳng hạn như thông qua triển khai khối quản lý bộ nhớ (memory management unit - MMU), MMU đầu vào/đầu ra hoặc MMU hệ thống, hoặc thông qua phía máy phụ thuộc chẳng hạn như thông qua triển khai khối bảo vệ bộ nhớ (memory protection unit - MPU) phía trước hệ thống con tốc độ dữ liệu gấp đôi (double data rate - DDR). Để triển khai cấu hình an toàn và truy cập vào bộ nhớ bởi SOC, SOC có thể bao gồm phần cứng và phần mềm để giám sát và bảo vệ truy cập bộ nhớ, đảm bảo các quy trình điều khiển truy cập bộ nhớ không cản trở hoặc làm giảm hiệu suất hệ thống và cung cấp các biện pháp bảo vệ để ngăn ngừa sự hư hỏng giữa các quá trình, rò rỉ, gây hại, và hoặc các cuộc tấn công bảo mật.

Các SOC mới đang được phát triển để mở rộng các trường hợp sử dụng, chẳng hạn như Internet vạn vật (Internet-of-Things - iot), thiết bị đeo được và các thiết bị có hệ số hình dạng nhỏ khác. Các trường hợp sử dụng như vậy có thể mang lại lợi ích khi giảm tải một số phần của phần cứng và/hoặc phần mềm từ SOC sang phần cứng và/hoặc các thiết bị bên ngoài để giảm kích thước vật lý, chi phí và mức tiêu thụ điện năng của SOC. Tuy nhiên, việc giảm tải phần cứng và phần mềm cho các thiết bị bên ngoài thường đã được triển khai cục bộ trong SOC có thể gây ra rủi ro bảo mật và suy giảm hiệu suất.

Bản chất kỹ thuật của sáng chế

Các khía cạnh khác nhau bao gồm các phương pháp và thiết bị nhớ triển khai các phương pháp để chỉ báo phản hồi về việc chấp nhận truy cập/vi phạm đối với SOC như là một phần của chuỗi giao dịch đọc/ghi của thiết bị nhớ bởi SOC. Các khía cạnh khác nhau có thể bao gồm bước nhận bản tin cấu hình từ SOC để tạo cấu hình điều khiển truy cập bộ

nhớ của thiết bị nhớ, tạo cấu hình điều khiển truy cập bộ nhớ dựa trên bản tin cấu hình, nhận bản tin yêu cầu truy cập từ SOC yêu cầu truy cập vào địa chỉ cơ sở của bộ nhớ và phạm vi truy cập bộ nhớ của mảng ô nhớ của thiết bị nhớ, trong đó bản tin yêu cầu truy cập có thể bao gồm hoạt động đọc/ghi, so sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ đã được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được cho phép hay không, và thực hiện hoạt động đọc/ghi để đáp lại việc xác định rằng bản tin yêu cầu truy cập được cho phép.

Trong một số khía cạnh, bản tin cấu hình có thể bao gồm ID miền bảo mật cấu hình, và bản tin yêu cầu truy cập có thể bao gồm ID miền bảo mật được yêu cầu. Trong một số khía cạnh, bản tin cấu hình có thể là bản tin JEDEC được mã hóa bao gồm ID miền bảo mật cấu hình, và bản tin yêu cầu truy cập có thể là bản tin JEDEC được mã hóa bao gồm ID miền bảo mật được yêu cầu. Trong một số khía cạnh, việc so sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ đã được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được cho phép hay không có thể bao gồm việc xác định xem ID miền bảo mật cấu hình có khớp với ID miền bảo mật được yêu cầu hay không, và để đáp lại việc xác định rằng ID miền bảo mật cấu hình khớp với ID miền bảo mật được yêu cầu, xác định rằng bản tin yêu cầu truy cập được cho phép, và truyền thông báo tới SOC cho biết rằng bản tin yêu cầu truy cập được cho phép. Các khía cạnh như vậy có thể còn bao gồm bước, để đáp lại việc xác định rằng ID miền bảo mật cấu hình không khớp với ID miền bảo mật được yêu cầu, xác định rằng bản tin yêu cầu truy cập không được cho phép, lưu trữ thông tin lỗi bao gồm địa chỉ cơ sở của bộ nhớ, phạm vi truy cập bộ nhớ và ID miền bảo mật được yêu cầu, truyền thông báo tới SOC cho biết rằng bản tin yêu cầu truy cập không được cho phép, và truyền thông tin lỗi tới SOC để đáp lại việc nhận được yêu cầu ngắt do lỗi từ SOC.

Một số khía cạnh có thể còn bao gồm bước nhận mật khẩu mở khóa từ SOC, xác định xem mật khẩu mở khóa nhận được có khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận được lưu trữ trong thiết bị nhớ hay không, và mở khóa logic cổng thiết bị nhớ để cho phép điều khiển truy cập bộ nhớ nhận bản tin cấu hình để đáp lại việc xác định rằng mật khẩu mở khóa nhận được khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận. Một số khía cạnh có thể còn bao gồm bước nhận, từ SOC, lệnh khóa được tạo cấu hình để thiết lập bit khóa trong thanh ghi của thiết bị nhớ, và thiết lập bit khóa để ngăn thay đổi cấu hình đối với điều khiển truy cập bộ nhớ đã được tạo cấu hình.

Các khía cạnh khác có thể bao gồm thiết bị bộ nhớ có bộ xử lý được tạo cấu hình để thực hiện các hoạt động của phương pháp bất kỳ trong số các phương pháp được tóm tắt ở trên. Các khía cạnh khác bao gồm thiết bị nhớ có phương tiện để thực hiện các chức năng của phương pháp bất kỳ trong số các phương pháp được tóm tắt ở trên.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo được đưa vào bản mô tả này và cấu thành một phần của bản mô tả này, minh họa các phương án ví dụ, và cùng với phần mô tả chung trên đây và phần mô tả chi tiết dưới đây, dùng để giải thích các đặc điểm của một số phương án.

Fig.1 là sơ đồ khối thành phần minh họa ví dụ về hệ thống máy tính 100 để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án.

Fig.2 là sơ đồ khối thành phần minh họa ví dụ về hệ thống máy tính 200 bao gồm cổng để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án.

Fig.3 là sơ đồ khối thành phần minh họa ví dụ về hệ thống máy tính 300 để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án.

Fig.4 là sơ đồ dòng quy trình minh họa phương pháp 400 để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án.

Fig.5 là sơ đồ khối thành phần minh họa ví dụ về hệ thống máy tính 500 bao gồm các đường giao dịch cấu hình và dữ liệu để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án.

Fig.6 là sơ đồ dòng quy trình minh họa phương pháp 600 để theo dõi các vi phạm truy cập của thiết bị nhớ trong an toàn theo một số phương án.

Fig.7 minh họa bản đồ bộ nhớ hệ thống 700 để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án.

Fig.8 là sơ đồ dòng quy trình minh họa phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án.

Fig.9 là sơ đồ dòng quy trình minh họa các hoạt động thay thế có thể được thực hiện bởi thiết bị nhớ như một phần của phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án.

Fig.10 là sơ đồ dòng quy trình minh họa các hoạt động thay thế có thể được thực hiện bởi thiết bị nhớ như một phần của phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án.

Fig.11 là sơ đồ dòng quy trình minh họa các hoạt động thay thế có thể được thực hiện bởi thiết bị nhớ như một phần của phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án.

Fig.12 là sơ đồ dòng quy trình minh họa các hoạt động thay thế có thể được thực hiện bởi thiết bị nhớ như một phần của phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án.

Fig.13 minh họa ví dụ về thiết bị điện toán đeo được ở dạng đồng hồ thông minh 1300 theo một số phương án.

Fig.14 là sơ đồ khối thành phần của ví dụ về thiết bị điện toán mạng 1400 có thể cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án.

Fig.15 là sơ đồ khối thành phần của ví dụ về thiết bị không dây ở dạng điện thoại thông minh 1500 phù hợp để triển khai một số phương án.

Mô tả chi tiết sáng chế

Các phương án khác nhau sẽ được mô tả chi tiết với tham chiếu tới các hình vẽ kèm theo. Bất cứ khi nào có thể, các số chỉ dẫn giống nhau sẽ được sử dụng trong toàn bộ hình vẽ để chỉ các bộ phận tương tự hoặc giống nhau. Các tham chiếu được đưa ra cho các ví dụ và phương án cụ thể là nhằm mục đích minh họa và không nhằm mục đích giới hạn phạm vi của các phương án khác nhau hoặc phần yêu cầu bảo hộ.

Các phương án khác nhau đem lại giải pháp cung cấp điều khiển truy cập thiết bị nhớ trong an toàn để cho phép giảm tải một số phần của phần cứng và/hoặc phần mềm sang thiết bị bên ngoài nhằm giảm kích thước, chi phí và mức tiêu thụ điện năng của SOC mà không gây ra rủi ro bảo mật và suy giảm hiệu suất.

Thuật ngữ "thiết bị không dây" được sử dụng ở đây để chỉ bất kỳ một hoặc tất cả các thiết bị bao gồm điện thoại di động, điện thoại thông minh, thiết bị điện tính xách tay, trình phát đa phương tiện cá nhân hoặc di động, xe tự hành, các bộ phận truyền thông không dây trong xe tự hành và bán tự hành, các thiết bị không dây được gắn hoặc được tích hợp vào các nền tảng di động khác nhau, điện thoại di động có tính năng Internet đa

phương tiện, và các thiết bị điện tử tương tự bao gồm bộ nhớ, các thành phần truyền thông không dây và bộ xử lý có thể lập trình.

Thuật ngữ "hệ thống trên chip" (system on chip - SOC) được sử dụng ở đây để chỉ một chip mạch tích hợp (integrated circuit - IC) chứa nhiều tài nguyên hoặc bộ xử lý được tích hợp trên một tấm nền. Một SOC có thể chứa hệ mạch có các chức năng kỹ thuật số, tương tự, tín hiệu trộn và tần số vô tuyến. Một SOC cũng có thể bao gồm số lượng bất kỳ các bộ xử lý chuyên dụng hoặc đa năng (bộ xử lý tín hiệu số, bộ xử lý môđem, bộ xử lý viđeo, v.v.), các khối bộ nhớ (chẳng hạn như ROM, RAM, Flash, v.v.), và các tài nguyên (chẳng hạn như bộ hẹn giờ, bộ ổn áp, bộ dao động, v.v.). Các SOC cũng có thể bao gồm phần mềm để điều khiển các tài nguyên và bộ xử lý tích hợp, cũng như để điều khiển các thiết bị ngoại vi.

Thuật ngữ "hệ thống trong gói" (system in a package - SIP) được sử dụng ở đây để chỉ một mođun hoặc gói có chứa nhiều tài nguyên, đơn vị tính toán, lõi hoặc bộ xử lý trên hai hoặc nhiều chip IC, tấm nền hoặc SOC. Ví dụ, SIP có thể bao gồm một tấm nền trên đó nhiều chip IC hoặc chip khuôn bán dẫn được xếp chồng lên nhau theo cấu hình thẳng đứng. Tương tự, SIP có thể bao gồm một hoặc nhiều mođun đa chip (multi-chip module - MCM) trên đó nhiều IC hoặc chip khuôn bán dẫn được đóng gói thành tấm nền hợp nhất. SIP cũng có thể bao gồm nhiều SOC độc lập được ghép nối với nhau qua hệ mạch truyền thông tốc độ cao và được đóng gói gần nhau, chẳng hạn như trên bảng mạch chủ đơn lẻ hoặc trong thiết bị không dây đơn lẻ. Việc các SOC ở gần nhau tạo điều kiện cho các cuộc truyền thông tốc độ cao và việc chia sẻ bộ nhớ và tài nguyên.

Trong các thiết bị điện toán thông thường, mạch và các thành phần điều khiển truy cập bộ nhớ được đặt về mặt vật lý bên trong các thiết bị điện toán đó. Ví dụ, để truy cập bộ nhớ truy cập ngẫu nhiên bên ngoài (RAM), SOC sẽ bao gồm các thành phần và mạch để điều khiển truy cập bộ nhớ trong bố trí vật lý của SOC sao cho việc truy cập RAM được kiểm soát bởi SOC.

Nhiều phương án triển khai điều khiển truy cập bộ nhớ an toàn trong thiết bị nhớ thay vì trong SOC. Các phương án khác nhau có thể bao gồm kích hoạt quyền điều khiển truy cập trong thiết bị nhớ, truyền tải miền bảo mật của bộ khởi tạo trong mỗi giao dịch tới bộ nhớ, thực thi điều khiển truy cập trong thiết bị nhớ bao gồm cấu hình, thực thi chính sách và chỉ báo lỗi, kiểm tra chỉ báo lỗi truy cập như là một phần của trình tự đọc/ghi và

thiết lập quyền điều khiển truy cập vào thiết bị nhớ như là một phần của trình tự khởi tạo hệ thống.

Các phương án khác nhau bao gồm các cơ chế bảo mật, chẳng hạn như cổng và cầu chì, trong SOC cho phép SOC tạo cấu hình điều khiển truy cập bộ nhớ nằm trong thiết bị nhớ nằm ngoài bố trí vật lý của SOC nhưng trong giao tiếp điện với SOC. Bằng cách giảm tải điều khiển truy cập bộ nhớ từ SOC sang thiết bị nhớ hoặc nhiều thiết bị, kích thước vật lý, chi phí và mức tiêu thụ điện năng của SOC có thể giảm. Các lợi ích bổ sung của việc triển khai điều khiển truy cập bộ nhớ trong thiết bị nhớ thay vì SOC bao gồm loại bỏ nhu cầu về các sơ đồ điều khiển truy cập độc quyền trên nhiều nhà cung cấp SOC và do đó tăng tiêu chuẩn hóa và khả năng truyền thông, cho phép sử dụng chip vi xử lý có độ phức tạp thấp hoặc trung bình theo cách an toàn hệ thống bộ nhớ, tái sử dụng chương trình cơ sở/phần mềm điều khiển truy cập trên nhiều bộ vi xử lý, bộ xử lý ứng dụng (application processor - AP) hoặc SOC và phát triển các thiết bị nhớ mới, phức tạp hơn (ví dụ: thiết bị điện toán trong/gần bộ nhớ) có khả năng bao gồm các chức năng như tính toán và điều khiển truy cập.

Fig.1 là sơ đồ khối thành phần minh họa hệ thống máy tính 100 ví dụ để cung cấp quyền điều khiển truy cập thiết bị nhớ trong an toàn thay vì bên trong SOC theo một số phương án. Các phương án khác nhau bao gồm triển khai khối phần cứng điều khiển truy cập bộ nhớ trong thiết bị nhớ, chẳng hạn như RAM 122 có thể được triển khai trong hệ thống giao tiếp điện với thiết bị xử lý (ví dụ: AP, SOC, SIP, v.v.). Các phương án khác nhau có thể được triển khai dưới dạng thiết bị nhớ, chẳng hạn như RAM động (dynamic RAM - DRAM), bộ nhớ lưu trữ, RAM không khả biến (non-volatile RAM - NVRAM) hoặc bất kỳ loại thiết bị nhớ hoặc mođun nào có thể giao tiếp điện với SOC 140 trong hệ thống.

SOC có thể được triển khai trong hệ thống có một hoặc nhiều thiết bị RAM an toàn. Do đó, các giao thức hoặc quy trình bắt tay bổ sung có thể được thực hiện để thiết lập mức độ bảo mật giữa SOC không an toàn và RAM an toàn. Ví dụ, các quy trình bổ sung có thể được thực hiện để thiết lập sự tin cậy giữa SOC 140 và RAM 122 trên bus 120 (ví dụ: bus tốc độ cao, bus RAM, v.v.). SOC có thể bao gồm chương trình tin cậy 102, bộ xử lý trung tâm (CPU) 104, RAM tĩnh (SRAM) 106, bộ nhớ chỉ đọc (ROM) 108, bộ điều khiển bộ nhớ RAM 110 bao gồm đầu cuối 112, giao diện điều khiển 114, và giao diện vật lý (PHY) 116, bộ điều khiển bộ nhớ lưu trữ 142 để truy cập bộ nhớ lưu trữ 144 và cầu chì

146. RAM 122 có thể bao gồm PHY 124 và mảng ô RAM 138. RAM 122 có thể còn bao gồm khối phần cứng tin cậy 125 bao gồm cổng 126 và cầu chì 128. RAM 122 có thể còn bao gồm khối phần cứng điều khiển truy cập 130 bao gồm khối cấu hình điều khiển truy cập 132, khối hội chứng vi phạm truy cập 134 và khối thực thi chính sách 136. SOC 140 có thể được ghép nối điện với PHY 124 của RAM 122 thông qua PHY 116 để giao tiếp các giao thức bắt tay nhằm cho phép SOC 140 định cấu hình khối phần cứng điều khiển truy cập 130. Khối phần cứng tin cậy 125, bao gồm cổng 126 và cầu chì 128, của RAM 122 có thể được triển khai để thiết lập tin cậy giữa SOC 140 và RAM 122. Khi tin cậy được thiết lập, SOC 140 sau đó có thể cấu hình khối phần cứng điều khiển truy cập 130 để cung cấp khả năng bảo vệ bộ nhớ theo các phương án khác nhau.

Trong một số phương án, khối phần cứng điều khiển truy cập 130 trong RAM122 có thể có chức năng tương tự như điều khiển truy cập thông thường về mặt vật lý trong SOC và có thể thực hiện các quy trình bao gồm kiểm tra bộ khởi tạo, miền bảo mật, địa chỉ vật lý và loại truy cập để xác định xem truy cập đọc hoặc ghi, sau đó cho phép truy cập bộ nhớ vào mảng ô RAM 138 cho các giao dịch được cho phép. Cổng 126 có thể được mở khóa trước khi khối phần cứng điều khiển truy cập 130 có thể được khởi tạo thông qua khối cấu hình điều khiển truy cập 132. Mở khóa có thể xảy ra khi chương trình tin cậy 102 chạy trên CPU 104 gửi mật khẩu mở khóa tới RAM 122, trong đó mật khẩu được kiểm tra dựa trên giá trị nằm trong cầu chì 128. Mật khẩu có thể là bí mật và có thể được cung cấp trước vào cầu chì RAM 128. Nếu mở khóa bằng mật khẩu thành công, cổng 126 có thể mở truy cập đọc/ghi vào khối cấu hình điều khiển truy cập 132 và chương trình tin cậy 102 có thể khởi tạo khối cấu hình điều khiển truy cập 132 như khi nó được chứa trong SOC theo các phương pháp thông thường. Sau khi hoàn tất quá trình khởi tạo, cổng 126 có thể trở về trạng thái khóa. Các thay đổi bổ sung đối với khối cấu hình điều khiển truy cập 132 có thể tuân theo quy trình mở khóa/thay đổi/khóa này mọi lúc. Khi khối phần cứng điều khiển truy cập 130 được khởi tạo, khối thực thi chính sách 136 có thể giám sát và điều chỉnh lưu lượng chế độ nhiệm vụ giữa SOC 140 và mảng ô RAM 138.

Fig.2 là sơ đồ khối thành phần minh họa ví dụ về hệ thống máy tính 200 hiển thị chi tiết về cổng 126 được ghép nối với logic 204 trong khối phần cứng tin cậy 125 được tạo cấu hình để cung cấp quyền điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án.

Tham chiếu đến các FIG.1 và 2, cổng 126 có thể bao gồm một hoặc nhiều cổng chấp nhận 202 và logic điều khiển 204. Cổng chấp nhận 202 có thể bao gồm một hoặc nhiều chuyển mạch nội tuyến kết nối/ngắt kết nối PHY 124 với khối phần cứng điều khiển truy cập 130 có thể cung cấp truy cập vào mảng ô RAM 138. Như đã đề cập ở trên, PHY 124 có thể cung cấp các kết nối được liên kết với bus 120. Kết nối 120d tương ứng với tín hiệu dữ liệu, và kết nối 120c tương ứng với tín hiệu địa chỉ/điều khiển. PHY 124 có thể cung cấp tín hiệu dữ liệu liên kết với các kết nối 120d đến các cổng chấp nhận 202 và logic điều khiển 204 của khối phần cứng tin cậy 125 thông qua các kết nối 214d. PHY 124 có thể cung cấp tín hiệu địa chỉ/điều khiển liên kết với các kết nối 120c đến các cổng chấp nhận 202 và logic điều khiển 204 của khối phần cứng tin cậy 125 thông qua các kết nối 214c.

Như được minh họa thêm trên Fig.2, mỗi cổng chấp nhận 202 có thể bao gồm tiếp điểm thứ nhất và tiếp điểm thứ hai. Tiếp điểm thứ nhất có thể được ghép nối điện với (các) kết nối dữ liệu tương ứng 214d và kết nối địa chỉ/điều khiển 214c, và tiếp điểm thứ hai ở phía bên kia của cổng hoặc công tắc có thể được ghép nối điện với (các) kết nối dữ liệu được kiểm soát tương ứng 216d và kết nối địa chỉ/điều khiển được kiểm soát 216c. Logic điều khiển 204 có thể được ghép điện với từng cổng chấp nhận 202 thông qua (các) kết nối 218 thông qua đó các tín hiệu điều khiển cổng có thể được cung cấp để mở và đóng các công tắc riêng lẻ. Về vấn đề này, "trạng thái bị khóa" của khối phần cứng tin cậy 125 có thể tương ứng với trạng thái hoạt động trong đó các cổng chấp nhận 202 được mở để ngăn truy cập vào các kết nối có cổng 216d và 216c.

Các phương án thay thế của chức năng cổng chấp nhận 202 có thể bao gồm bộ thu phát hai chiều với đầu ra được điều khiển bởi bộ điều khiển cổng 218, bộ thu phát hai chiều có thể được bật/tắt thông qua ray điện dưới sự điều khiển của bộ điều khiển cổng 218, hoặc thanh ghi/chốt khóa hai chiều có thể kích hoạt đầu ra hoặc ray điện dưới sự kiểm soát của bộ điều khiển cổng 218. Các mạch được sử dụng có thể được thiết kế có mục đích để báo hiệu hai chiều hoặc có thể bao gồm hai mạch riêng biệt để xử lý từng hướng (ví dụ: tiến và lùi) tương ứng với lưu lượng ghi và đọc dữ liệu.

Trong một số phương án, khi thiết bị nhớ 122 bị tắt nguồn, logic điều khiển 204 có thể nhận lệnh tương ứng từ bộ điều khiển quản lý nguồn điện của SOC 140 và để đáp lại, gửi tín hiệu điều khiển cổng "khóa" qua (các) kết nối 218 đến cổng chấp nhận 202. Các tín hiệu điều khiển cổng có thể bao gồm các tín hiệu riêng lẻ (ví dụ: một dây điều khiển cổng

cho một cổng chấp nhận) hoặc tín hiệu duy nhất (ví dụ: một cổng điều khiển cho tất cả các cổng chấp nhận). Trong một số phương án, cổng chấp nhận 202 có thể được thay thế bằng chuyển mạch nguồn để bật hoặc tắt nguồn khối phần cứng điều khiển truy cập 130 đến mảng ô RAM 138. Để đáp lại việc tín hiệu điều khiển cổng "khóa", cổng chấp nhận 202 có thể được mở để ngăn truy cập vào các kết nối kiểm soát 216d và 216c. Theo cách này, khi thiết bị nhớ được khởi động, cơ chế cổng 126 ở "trạng thái khóa" với các cổng chấp nhận 202 ở vị trí mở để ban đầu ngăn các thao tác đọc/ghi truy cập vào mảng ô nhớ RAM 138.

Như được mô tả có tham chiếu đến Fig.1, khi hệ thống 200 khởi động và chương trình tin cậy 102 bắt đầu thực thi trên CPU 104, mật khẩu mở khóa được lưu trữ trong (các) cầu chì 146 trên SOC 140 có thể được tìm nạp và cung cấp cho bộ điều khiển 110, bộ điều khiển này sẽ truyền giá trị qua PHY 116 đến PHY 124. Logic điều khiển 204 trong khối phần cứng tin cậy 125 có thể tìm nạp giá trị cổng chấp nhận được cung cấp trong (các) cầu chì 128 thông qua, ví dụ: bus dữ liệu cầu chì 220 và bus điều khiển cầu chì 222 trong khối phần cứng tin cậy 125. Như được minh họa trên Fig.2, khối phần cứng tin cậy 125 và/hoặc (các) cầu chì 128 có thể bao gồm bộ điều khiển 212 để tạo điều kiện giao tiếp với logic điều khiển 204. Logic điều khiển 204 có thể so sánh giá trị cổng chấp nhận với mật khẩu mở khóa nhận được từ SOC 140. Nếu mật khẩu mở khóa khớp với giá trị cổng chấp nhận, logic điều khiển 204 có thể gửi tín hiệu điều khiển cổng "mở khóa" đến cổng chấp nhận 202 qua (các) kết nối 218. Để đáp lại việc tín hiệu điều khiển cổng "mở khóa", các cổng chấp nhận 202 có thể bị đóng, do đó kết nối (các) kết nối dữ liệu 214d và kết nối địa chỉ/điều khiển 214c với (các) kết nối kiểm soát 216d và kết nối địa chỉ/điều khiển kiểm soát 216c tương ứng. Ở "trạng thái mở khóa" này, cơ chế cổng 126 có thể cung cấp truy cập không hạn chế vào khối phần cứng điều khiển truy cập 130 qua bus dữ liệu 224d và bus điều khiển 224c.

Như đã đề cập ở trên, việc trao đổi mật khẩu giữa SOC 140 và RAM kiểm soát 122 có thể được triển khai theo nhiều cách khác nhau. Trong một số phương án, việc trao đổi mật khẩu không được mã hóa đơn giản có thể được thực hiện thông qua (các) cầu chì 146, 128. Trong một số phương án, trao đổi mật khẩu an toàn có thể sử dụng (các) thuật toán mã hóa mong muốn bất kỳ để cải thiện mức độ bảo mật thông qua các quy trình hoặc giao thức bắt tay phức tạp hơn hoặc bổ sung. Như được minh họa trên Fig.2, khi quá trình trao đổi mật khẩu an toàn sử dụng mã hóa, logic điều khiển 204 trong khối phần cứng tin cậy

125 có thể bao gồm các mođun logic để hỗ trợ hàm giải mã (khối 206), hàm băm (khối 208) và hàm kiểm tra (khối 210).

Logic giải mã 206 trong khối phần cứng tin cậy 125 có thể nhận thông tin điều khiển và địa chỉ qua bus 214c và dữ liệu qua bus 214d. Trong một số phương án, giao thức được xác định trước và/hoặc được chuẩn hóa có thể được triển khai để kiểm soát logic điều khiển 204, trao đổi thông tin như các khóa và mật khẩu hoặc khởi tạo và lập trình các phần tử như cầu chì 128. Ví dụ, có thể có lệnh cụ thể trên bus địa chỉ và điều khiển 214d có thể được giải mã bằng logic giải mã 206 và sau đó có thể khởi tạo chức năng lệnh cụ thể. Một số phương án có thể bao gồm lệnh và dữ liệu duy nhất được liên kết với từng loại hàm, chẳng hạn như logic cổng đặt lại, dữ liệu cầu chì chương trình ở nhiều vị trí, khóa riêng của chương trình, mật khẩu chương trình, lần thử tự hủy chương trình không thành công, cơ chế kích hoạt giả mạo, mođun khóa đầu vào p, cơ sở khóa đầu vào g, hàm băm truy xuất, mở khóa mật khẩu không được mã hóa, mở khóa mật khẩu được mã hóa, v.v.

Logic giải mã 206 trong khối phần cứng tin cậy 125 có thể chịu trách nhiệm phân tích cú pháp và kích hoạt các hoạt động thích hợp để đáp lại các điều khiển, địa chỉ và dữ liệu đi đến. Như được minh họa trên Fig.2, kết nối điều khiển và địa chỉ 214c và dữ liệu 214d đến cổng thông tin qua 202 và nếu được mở khóa, có thể chuyển đến phần cứng kiểm tra giám sát truy cập 130, khối này có thể thực hiện các hoạt động chế độ tiêu chuẩn hóa tương tự và/hoặc đã được xác định trước, như đọc mảng ô RAM, ghi mảng ô RAM, chọn trang mảng ô RAM, sửa mảng ô RAM, cấu hình thiết bị RAM, cấu hình nâng cao PHY và bất kỳ chức năng nào khác không liên quan đến các chức năng chống giả mạo.

Hàm băm 208 có thể thực hiện các phép toán số học mođun cho quy trình trao đổi khóa bí mật và có thể bao gồm các bảng tra cứu và/hoặc logic tính toán tuần tự và song song phép cộng mođun. Hàm kiểm tra 210 có thể được bao gồm trong logic điều khiển 204 của khối phần cứng tin cậy 125 để so sánh mật khẩu được gửi từ SOC 140 với bản sao cục bộ đã được lập trình trước đó trong cầu chì cục bộ 128 trong khối phần cứng tin cậy 125. Logic giải mã (không được thể hiện) có thể được bao gồm trong hàm kiểm tra 210 của khối phần cứng tin cậy 125 để cho phép SOC 140 gửi mật khẩu bằng cách mã hóa nhằm ngăn kẻ rình mò xem mật khẩu khi mật khẩu di chuyển qua bus bên ngoài 120. Nếu SOC 140 đã mã hóa mật khẩu, thì logic giải mã trước tiên có thể giải mã mật khẩu bằng khóa bí mật dùng chung có được trong quá trình trao đổi an toàn, chẳng hạn như phương pháp Diffie-Hellman.

Trong một số phương án, trong trường hợp xảy ra nhiều sự kiện mở khóa không thành công, các cầu chì 128 trong khối phần cứng tin cậy 125 có thể được kích hoạt để vô hiệu hóa vĩnh viễn logic điều khiển 204, do đó ngăn truy cập vào bộ nhớ trong tương lai.

Fig.3 là sơ đồ khối thành phần minh họa ví dụ về hệ thống máy tính 300 để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án. Liên quan đến các FIG.1-3, SOC 140 có thể bao gồm các đơn vị xử lý triển khai các chương trình tin cậy khác nhau ngoài chương trình tin cậy 102 do CPU 104 triển khai. Ví dụ, SOC 140 có thể bao gồm bộ xử lý mạng (NPU) 308 thực hiện chương trình tin cậy 306 trong đó NPU 308 được kết nối điện với bus 118.

SOC 140 trong giao tiếp điện với RAM 122 có thể cấu hình khối phần cứng điều khiển truy cập 130 mỗi khi SOC thực hiện nỗ lực truy cập mới mảng ô RAM 138. Trước khi tạo cấu hình khối phần cứng điều khiển truy cập 130, SOC 140 và RAM 122 có thể được khởi tạo để tạo cấu hình lọc truy cập bộ nhớ ở chế độ nhiệm vụ. Ví dụ, trao đổi khóa và thiết lập kênh an toàn có thể được thực hiện trước khi SOC 140 tạo cấu hình và khởi tạo khối phần cứng điều khiển truy cập 130. Thực thể hoặc thành phần an toàn của SOC 140 có thể bao gồm khóa hoặc mật khẩu để mở cổng 126. Như được mô tả ở trên, SOC 140 có thể truyền khóa tới RAM 122 để mở cổng 126, sau đó cho phép SOC 140 cấu hình khối phần cứng điều khiển truy cập 130 để khởi tạo truy cập thích hợp vào mảng ô RAM 138. Sau khi tạo cấu hình khối phần cứng điều khiển truy cập 130, SOC 140 có thể thiết lập bit khóa trong RAM 122 để ngăn sửa đổi thêm đối với khối phần cứng điều khiển truy cập 130. Thực thể bảo mật của SOC 140 cũng có thể đưa ra các lệnh cho khối phần cứng điều khiển truy cập 130 để thay đổi lại cấu hình cho các lần thử truy cập bộ nhớ tiếp theo trong tương lai sau khi trao đổi thông tin bộ nhớ qua kênh bảo mật đã thiết lập. Nói cách khác, SOC 140 có thể mở khóa cổng 126 bằng cách sử dụng khóa hoặc mật khẩu/mật mã được lưu trữ trong thực thể an toàn của SOC 140, cấu hình khối phần cứng điều khiển truy cập 130 bằng thông tin truy cập bộ nhớ thích hợp, khóa cấu hình để ngăn sửa đổi kênh bảo mật trong khi việc truy cập vào mảng ô RAM 138 đang diễn ra và kích hoạt khối phần cứng điều khiển truy cập 130 để bắt đầu truy cập mảng ô RAM 138 sau khi kênh bảo mật đã được tạo cấu hình và khóa.

RAM 122 có thể cung cấp các giao diện thanh ghi để điều khiển bên bởi SOC 140. RAM 122 có thể bao gồm bit khóa cho từng vùng truy cập trong mảng ô RAM 138 để ngăn việc sửa đổi thêm cấu hình. Các bit khóa có thể được đặt, bật hoặc được tạo cấu hình

khác sau khi khởi tạo SOC-RAM để khóa trong cấu hình gần nhất của khối phần cứng điều khiển truy cập 130. RAM 122 có thể bao gồm bit kích hoạt cho từng vùng truy cập của mảng ô RAM 138, sao cho việc đặt bit kích hoạt cho phép thực thi (ví dụ: thông qua khối thực thi chính sách 136) của khối phần cứng điều khiển truy cập được tạo cấu hình 130.

SOC 140 có thể cấu hình khối phần cứng điều khiển truy cập 130 để truy cập các phần hoặc miền cụ thể của mảng ô RAM 138 bằng cách mã hóa thông tin truy cập trong lệnh được gửi tới RAM 122. Ví dụ, SOC 140 có thể mã hóa thông tin liên quan đến địa chỉ cơ sở của bộ nhớ (ví dụ: addr 32), kích thước và/hoặc phạm vi dữ liệu bộ nhớ (ví dụ: dữ liệu 34) và ID miền truy cập (ví dụ: ID 36) trong lệnh được truyền tới RAM 122 thông qua các kênh dữ liệu và truy cập/điều khiển (ví dụ: các kết nối 120d, 120c, 214d, 214c, 216d, 216c). Thông tin kích thước và địa chỉ cơ sở cho từng vùng truy cập có thể được biểu thị theo sơ đồ truy cập thiết bị nhớ, chẳng hạn như ở mức độ chi tiết của các hàng ô nhớ của mảng ô RAM 138. Trong một số ví dụ, ID miền truy cập/ID miền bảo mật có thể được truyền tới RAM 122 qua bus tách biệt với dữ liệu và các kênh truy cập/điều khiển. Ví dụ, bộ điều khiển bộ nhớ RAM 110 có thể truyền ID miền bảo mật tới PHY 124 và sau đó tới khối phần cứng điều khiển truy cập 130 qua các kết nối 302i và 304i.

Lệnh mã hóa có thể bao gồm thông tin để truy cập cấu hình chính xác cho từng vùng hoặc miền truy cập. Lệnh mã hóa có thể bao gồm ID bảo mật hoặc ID miền, và khối thực thi chính sách 136 có thể kiểm tra ID bảo mật để xác minh miền nào mà SOC 140 đang cố gắng truy cập. Lệnh mã hóa cũng có thể bao gồm thông tin để chỉ rõ sự cho phép truy cập đọc và ghi cho từng miền bảo mật được hỗ trợ của mảng ô RAM 138. Nói cách khác, lệnh mã hóa có thể chỉ định đọc thông tin bộ nhớ từ miền bảo mật, ghi thông tin bộ nhớ vào miền bảo mật hoặc cả đọc và ghi vào miền bảo mật. Ví dụ, RAM 122 có thể hỗ trợ bốn miền bảo mật có thể được ánh xạ tới bốn miền bảo mật bên SOC 140: AP, Đồ họa, xử lý tín hiệu số (DSP) và bộ xử lý bảo mật. Đối với mỗi vùng điều khiển truy cập, có thể có bốn bit để biểu thị quyền đọc đối với từng miền bảo mật và bốn bit để biểu thị quyền ghi đối với từng miền bảo mật. SOC 140 có thể cấu hình cách ID miền bảo mật được ánh xạ tới miền bảo mật SOC 140. Ví dụ, SOC 140 có thể xác định hoặc phân bổ giá trị ID bảo mật bằng 0 cho hệ điều hành mức cao AP (HLOS), 1 cho thực thể bảo mật AP, 2 cho đồ họa và 3 cho bộ xử lý bảo mật. Các cấp phép truy cập đọc/ghi có thể được chỉ rõ trong lệnh mã hóa cho từng miền bảo mật cụ thể trong mảng ô RAM 138.

Trong một số phương án, khối hội chứng vi phạm truy cập 134 của khối phần cứng điều khiển truy cập 130 có thể theo dõi và báo cáo bất kỳ lỗi nào xảy ra trước và trong khi tạo cấu hình điều khiển truy cập cũng như trong quá trình trao đổi bộ nhớ qua và thiết lập kênh an toàn sau khi khối phần cứng điều khiển truy cập 130 được tạo cấu hình. RAM 122 có thể bao gồm chân ngắt lỗi có thể truyền tín hiệu ngắt tới SOC 140 khi lỗi được phát hiện bởi khối hội chứng vi phạm truy cập 134. Ví dụ, khối hội chứng vi phạm truy cập có thể quan sát thấy rằng một hoặc nhiều lỗi đã xảy ra trong quá trình truy cập bộ nhớ (ví dụ: đọc từ và/hoặc ghi vào các miền bảo mật trong mảng ô RAM 138) sau khi khối phần cứng điều khiển truy cập 130 đã được tạo cấu hình phù hợp . Để đáp lại việc quan sát và ghi lại (các) lỗi, điều khiển truy cập sau đó có thể gửi tín hiệu ngắt lỗi tới bộ điều khiển bộ nhớ RAM 110 của SOC 140 từ PHY 124 thông qua các kết nối 304e và 302e. Chỉ báo lỗi/tín hiệu ngắt/chân (ví dụ: kết nối 302e) có thể được nhận biết bởi SOC 140 ít nhất một chu kỳ đồng hồ sau khi lệnh đọc hoặc ghi được thực thi. Đối với các lỗi đọc, chỉ báo lỗi có thể là phần của phản hồi đọc, sao cho phản hồi đọc có thể bao gồm giá trị không xác định trên bus dữ liệu (ví dụ: kết nối 120d). Đối với các lỗi ghi, có thể cần thêm một chu kỳ đồng hồ để nhận biết chân ngắt lỗi, do đó khối hội chứng vi phạm truy cập 134 có thể phân tích xem lệnh ghi có được thực hiện không chính xác hoặc không thể được thực thi đúng cách hay không, sau đó tạo ra chỉ báo để truyền tới SOC 140 cho biết rằng lệnh ghi dẫn đến một hoặc nhiều lỗi. Chỉ báo lỗi được tạo bởi khối hội chứng vi phạm truy cập 134 có thể bao gồm loại lỗi (ví dụ: lỗi đọc/ghi), địa chỉ lỗi tương ứng với mảng ô RAM 138 và ID miền bảo mật mà lỗi tương ứng. Ví dụ, ID miền bảo mật được báo cáo trong tín hiệu ngắt lỗi có thể xác định miền bảo mật nào (ví dụ: AP HLOS, thực thể bảo mật AP, đồ họa, bộ xử lý bảo mật, v.v.) Của SOC 140 đang cố truy cập mảng ô RAM 138 khi (các) lỗi xảy ra.

Chỉ báo lỗi có thể bao gồm thông tin này cho một hoặc nhiều lỗi xảy ra do hoạt động đọc hoặc ghi. Ví dụ, khối hội chứng vi phạm truy cập 134 có thể lưu trữ loạt lỗi có thể đã xảy ra trước khi SOC 140 được bấm đồng hồ để nhận biết ít nhất một trong các lỗi đã xảy ra. Do đó, việc tạo bộ đệm lỗi thông qua khối hội chứng vi phạm truy cập 134 có thể cho phép SOC 140 nhận được báo cáo toàn diện về các lỗi trong một chu kỳ đồng hồ mà không bỏ sót bất kỳ lỗi nào có thể xảy ra trong một hoặc nhiều chu kỳ đồng hồ trước lỗi được quan sát gần nhất. Trong một số phương án, chỉ báo lỗi được báo cáo cho SOC 140 có thể bao gồm chỉ báo về vị trí lệnh truy cập bộ nhớ có thể đã bị từ chối dọc theo kết nối dữ liệu và/hoặc điều khiển tại khối cấu hình điều khiển truy cập 132, khối thực thi

chính sách 136 và mảng ô RAM 138. Trong một số ví dụ, khối hội chứng vi phạm truy cập 134 có thể bao gồm bộ đếm đếm số lỗi đã xảy ra từ một hoặc nhiều lệnh truy cập bộ nhớ.

Fig.4 là sơ đồ dòng quy trình minh họa phương pháp 400 để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án. Tham chiếu đến các hình vẽ Fig.1-4, các hoạt động của phương pháp 400 có thể được thực hiện bởi bộ xử lý (ví dụ: CPU 104, NPU 308) của SOC (ví dụ: SOC 140) tạo cấu hình thiết bị nhớ ngoài (ví dụ: RAM 122).

Thứ tự của các hoạt động được thực hiện trong các khối 402-418 chỉ mang tính minh họa và các hoạt động của các khối 402-418 có thể được thực hiện theo thứ tự bất kỳ và một phần xảy ra đồng thời trong một số phương án. Trong một số phương án, phương pháp 400 có thể được thực hiện bởi bộ xử lý của thiết bị độc lập với, nhưng kết hợp với, thiết bị nhớ ngoài. Ví dụ, phương pháp 400 có thể được triển khai dưới dạng mođun phần mềm thực thi trong bộ xử lý của SOC hoặc trong phần cứng chuyên dụng trong SOC đưa ra các lệnh để thiết lập các kênh bộ nhớ an toàn và bộ nhớ truy cập của thiết bị nhớ ngoài và được tạo cấu hình khác để thực hiện các hành động và lưu trữ dữ liệu như mô tả.

Trong khối 402, việc truy cập vào thiết bị nhớ có thể bị ngắt. Mặc định, thiết bị nhớ được thiết kế để có điều khiển truy cập an toàn trong bộ nhớ có thể ở trạng thái bị ngắt, trong đó thiết bị nhớ có thể được tạo cấu hình bởi thiết bị xử lý bên ngoài chẳng hạn như SOC. Ví dụ, như được mô tả thêm dựa vào các Fig.1-3, thiết bị nhớ có thể là RAM 122, có thể có cổng chấp nhận 202 ở trạng thái mở để cho bất kỳ thiết bị xử lý nào (ví dụ: SOC 140) sẽ không có truy cập vào bộ nhớ (ví dụ: mảng ô RAM 138) khi được ghép nối/ghép nối điện với RAM 122. Điều kiện ban đầu của thiết bị nhớ cũng có thể có các giá trị mặc định cho khóa/mật khẩu/mật khẩu không được khởi tạo hoặc lập trình theo cách khác sao cho khóa riêng có thể có trạng thái mặc định là trống/không được lập trình hoặc giá trị mặc định là 0. Ví dụ, cầu chì 128 của RAM 122 có thể có giá trị khóa riêng mặc định là 0.

Trong khối 404, SOC và thiết bị nhớ có thể được ghép cặp. Quá trình khởi tạo ban đầu có thể xảy ra trước khi triển khai hiện trường của hệ thống bao gồm SOC và thiết bị nhớ ngoài, chẳng hạn như SOC và thiết bị nhớ được lập trình với hoặc cấp các khóa/mật khẩu/mật mã cụ thể để cho phép thiết lập các kênh truy cập an toàn giữa SOC và thiết bị nhớ. Quá trình khởi tạo có thể bao gồm ghi (các) khóa riêng, (các) mật khẩu và một số lần thử truy cập tối đa trước khi khóa SOC khỏi thiết bị nhớ. Ví dụ, sau một số nỗ lực truy cập

không thành công của SOC, thiết bị nhớ có thể vô hiệu hóa điều khiển truy cập (ví dụ: bằng cách ngăn chặn thay đổi trạng thái của cổng/giữ cổng ở trạng thái mở khóa), ngăn chặn các cuộc tấn công lấy cắp dữ liệu tiềm tàng của SOC trái phép trong giao tiếp điện với thiết bị nhớ.

Trong khối 406, hệ thống bao gồm SOC và thiết bị nhớ ngoài ghép cặp có thể được khởi động. Quá trình khởi động hệ thống có thể bao gồm ghép cặp vật lý SOC và thiết bị nhớ (tức là trong hệ thống gắn cứng) rồi bật nguồn hệ thống. Ví dụ, SOC 140 có thể được nối dây cứng với RAM 122 để cho SOC 140 và RAM 122 được đặt vật lý và được ghép nối trong vỏ hệ thống.

Trong khối 408, khi SOC và thiết bị nhớ được cấp nguồn và khởi động, SOC có thể trao đổi thông tin khóa/mật khẩu với khối phần cứng tin cậy 125 của thiết bị nhớ như được mô tả với tham chiếu đến Fig.2. Thiết bị nhớ đang ở trạng thái khóa mặc định, khối phần cứng tin cậy 125 có thể nhận thông tin khóa/mật khẩu từ SOC và logic 204 có thể so sánh thông tin khóa/mật khẩu nhận được với thông tin được lưu trữ trong bộ nhớ cầu chì (fuse memory) 128 để xác minh xem SOC có quyền tạo cấu hình chính sách điều khiển truy cập của khối phần cứng điều khiển truy cập 130 của thiết bị nhớ. Nếu logic 204 xác minh quyền SOC, thì khối phần cứng tin cậy 125 có thể sau đó mở khóa cổng 126 để SOC tạo cấu hình điều khiển truy cập của khối phần cứng điều khiển truy cập 130. SOC có thể chọn ngẫu nhiên từ một bộ khóa chung để truyền tới thiết bị nhớ nhằm cho phép thiết bị nhớ xác định có cấp phép truy cập hay không. Bộ khóa công khai có thể được tạo cấu hình và lưu trữ bởi SOC như được mô tả trong khối 404.

Trong khối xác định 410,logic 204 của khối phần cứng tin cậy 125 có thể xác định thông tin chính do SOC cung cấp có hợp lệ hay không. Trong một số phương án,logic 204 của khối phần cứng tin cậy 125 có thể xác định khóa có hợp lệ trong khối xác định 410 hay không bằng cách so sánh với thông tin khóa riêng được khởi tạo trong thiết bị nhớ theo quy trình được mô tả trong khối 404. Như được mô tả có tham chiếu đến Fig.2, như được xác định bởi logic điều khiển 204 của khối phần cứng tin cậy 125, thiết bị nhớ sẽ vẫn ở trạng thái khóa (tức là cổng mở) nếu khóa do SOC truyền không hợp lệ hoặc thiết bị nhớ sẽ chuyển sang trạng thái mở khóa (tức là cổng đã đóng) nếu khóa hợp lệ.

Để đáp lại việc xác định rằng khóa do SOC cung cấp là không hợp lệ (nghĩa là khối xác định 410 = "Không"), SOC có thể thử truy cập thêm bằng cách chọn các khóa công

khai khác như được mô tả trong khối 408 cho đến khi một số lần cố gắng truy cập nhất định có thể xảy ra và thiết bị nhớ vẫn ở trạng thái bị khóa.

Để đáp lại việc xác định rằng khóa do SOC cung cấp là hợp lệ (nghĩa là khối xác định 410 = "Có"), khối phần cứng tin cậy 125có thể mở khóa để thiết lập kết nối an toàn với SOC và cho phép SOC truy cập vào phần cứng điều khiển truy cập khối 130 cho các mục đích cấu hình trước khi đưa ra các lệnh đọc/ghi vào bộ nhớ (ví dụ: mảng ô RAM 138) trong khối 412. Quá trình này có thể được thực hiện bởi SOC và thiết bị nhớ được ghép nối như được mô tả có tham chiếu đến Fig.2. Trong một số phương án, việc cấp phép truy cập bởi SOC có thể bao gồm mở khóa các thanh ghi của thiết bị nhớ để tạo cấu hình điều khiển truy cập.

Trong khối 414, SOC có thể gửi các lệnh đến thiết bị nhớ để tạo cấu hình và sau đó khóa điều khiển truy cập bộ nhớ của khối phần cứng điều khiển truy cập 130. Như được mô tả với tham chiếu đến Fig.3, SOC có thể đưa ra các lệnh mã hóa cho thiết bị nhớ để tạo cấu hình điều khiển truy cập của khối phần cứng điều khiển truy cập 130) để chuẩn bị thực hiện các hoạt động đọc/ghi bộ nhớ trên kênh bảo mật. Các lệnh mã hóa do SOC truyền và nhận bởi khối cấu hình điều khiển truy cập của thiết bị nhớ có thể bao gồm các tham số cấu hình truy cập bao gồm địa chỉ cơ sở, kích thước hoặc dải địa chỉ và ID miền bảo mật để xác định thực thể bảo mật nào của SOC đang cố gắng truy cập vào các phần cụ thể của bộ nhớ và bộ nhớ nào và bao nhiêu bộ nhớ sẽ được truy cập trong thiết bị nhớ. Bộ xử lý của SOC có thể đưa ra các hoạt động đọc/ghi cho khối cấu hình điều khiển truy cập 132 trong khối phần cứng điều khiển truy cập 130 để chuẩn bị kênh an toàn để trao đổi thông tin bộ nhớ.

Trong một số phương án, các lệnh đọc/ghi có thể được truyền tới thiết bị nhớ từ SOC theo các tiêu chuẩn bộ nhớ JEDEC. Ví dụ, việc triển khai các tiêu chuẩn JEDEC có thể bao gồm việc truyền các lệnh đọc/ghi qua bus JEDEC CMD và DATA, trong đó cmd opcode* chỉ rõ hoạt động là đọc hay ghi. Ví dụ, bảng 1 và 2 minh họa lệnh ghi để tạo cấu hình không gian địa chỉ của khối cấu hình điều khiển truy cập nhằm xác định các tham số cấu hình truy cập (ví dụ: địa chỉ cơ sở, dải địa chỉ, ID miền bảo mật) bằng cách sử dụng tiêu chuẩn JEDEC trong đó đọc, ghi, Cas-2, MRW-1 và MRW-2 (ghi thanh ghi chế độ) là các lệnh JEDEC hiện có. Ghi Đặc biệt và Cas-2 Đặc biệt có thể là các lệnh được sửa đổi các lệnh giao thức JEDEC được sử dụng để lập trình không gian thanh ghi của khối cấu hình điều khiển truy cập của thiết bị nhớ.

Bảng 1

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Ghi đặc biệt		*cmd**	*cmd**	*cmd**					1
									2

Bảng 2

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2 Đặc biệt		*cmd**	*cmd**	*cmd**					1
									2

Bởi vì SOC thực thi các lệnh như trong bảng 1 và 2, 32 byte không gian thanh ghi của cấu hình điều khiển truy cập được tạo cấu hình để xác định các tham số cấu hình truy cập. Các lệnh được hiển thị trong bảng 1 và 2 có thể được lặp lại nhiều lần khi cần để tạo cấu hình các không gian địa chỉ bổ sung trong khối cấu hình điều khiển truy cập cho từng miền bảo mật.

Trong một số phương án, các giao thức JEDEC có thể được sử dụng ở nhiều định dạng khác nhau tùy thuộc vào ứng dụng của hệ thống bao gồm SOC và thiết bị nhớ, sao cho thiết bị nhớ có thể được chuẩn hóa hoặc dành riêng cho ứng dụng. Ví dụ, bảng 3 và 4 minh họa loạt các lệnh để định cấu hình không gian địa chỉ của khối cấu hình điều khiển truy cập để xác định các tham số cấu hình truy cập bằng cách sử dụng các lệnh JEDEC hiện có.

Bảng 3

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Ghi		*cmd**	*cmd**	*cmd**					1
									2

Bảng 4

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2		*cmd**	*cmd**	*cmd**					1
									2

Ngoài các lệnh được thể hiện trong bảng 3 và 4, SOC có thể truyền lệnh tới khối cấu hình điều khiển truy cập trong khối phần cứng điều khiển truy cập 130 của thiết bị nhớ chỉ định địa chỉ cấu hình truy cập sẽ được sửa đổi. Ví dụ, SOC có thể truyền lệnh 32 byte

bao gồm 8 byte dữ liệu xác định địa chỉ cấu hình truy cập và 24 byte dữ liệu xác định các tham số cấu hình truy cập. Lệnh này có thể được truyền song song, đồng thời hoặc về cơ bản là cùng thời điểm SOC thực thi lệnh Cas-2, sao cho khối cấu hình điều khiển truy cập trong khối phần cứng điều khiển truy cập 130 của thiết bị nhớ có thể liên kết Ghi và Cas-2 với địa chỉ cấu hình truy cập nhận được và thông tin tham số. Như vậy, khối cấu hình điều khiển truy cập trong khối phần cứng điều khiển truy cập 130 có thể được tạo cấu hình để theo dõi cụ thể việc nhận lệnh bao gồm địa chỉ cấu hình truy cập và thông tin tham số trên một giao diện bus khi nhận lệnh Cas-2 trên giao diện bus khác. Các lệnh được hiển thị trong bảng 3 và 4 có thể được lặp lại nhiều lần khi cần để tạo cấu hình các không gian địa chỉ bổ sung trong khối cấu hình điều khiển truy cập cho từng miền bảo mật.

Bảng 1-4 chỉ minh họa một ví dụ cho phép SOC ghi các tham số cấu hình truy cập vào không gian địa chỉ của khối cấu hình điều khiển truy cập. Lệnh đọc có thể được thực thi để đọc thông tin tham số cấu hình truy cập từ không gian thanh ghi của khối cấu hình điều khiển truy cập trong khối phần cứng điều khiển truy cập 130 theo cách tương tự như lệnh ghi (nghĩa là thay thế "ghi" bằng "đọc" trong các lệnh JEDEC trong bảng 1-4).

SOC có thể cấu hình các tham số cấu hình truy cập bằng cách ghi vào các không gian địa chỉ cụ thể với khối cấu hình điều khiển truy cập trong khối phần cứng điều khiển truy cập 130 của thiết bị nhớ, như được mô tả ở trên. Các tham số cấu hình truy cập có thể xác định các loại truy cập được cho phép do SOC thực hiện sau khi tạo cấu hình điều khiển truy cập được thiết lập và khóa để thiết lập kênh an toàn giữa SOC và thiết bị nhớ. Ví dụ, SOC có thể thực hiện các hoạt động đọc và ghi tương ứng với địa chỉ cơ sở, dải địa chỉ và ID miền bảo mật như được tạo cấu hình trước đó trong điều khiển truy cập của khối phần cứng điều khiển truy cập 130. Nếu SOC cố gắng đưa ra yêu cầu đọc hoặc ghi dữ liệu vào miền bảo mật không được xác định khi tạo cấu hình các tham số cấu hình truy cập, thì khối phần cứng điều khiển truy cập 130 sẽ ghi lại lỗi và gửi ngắt đến SOC bao gồm thông tin liên quan đến lỗi (nghĩa là như được mô tả với tham chiếu đến khối hội chứng vi phạm truy cập 134 của Fig.3).

Sau khi điều khiển truy cập của khối phần cứng điều khiển truy cập 130 đã được tạo cấu hình theo các lệnh do SOC đưa ra, SOC cũng có thể đưa ra các lệnh cho khối phần cứng điều khiển truy cập 130 của thiết bị nhớ để thiết lập bit khóa thành khóa cấu hình điều khiển truy cập hiện tại để ngăn sửa đổi cấu hình. Trong một số phương án, SOC có thể đưa ra lệnh cho bộ nhớ để bỏ thiết lập bit khóa nhằm cho phép thay đổi cấu hình điều

khiển truy cập, như để thực hiện các thay đổi chính sách mới hoặc các thay đổi bộ nhớ. SOC cũng có thể ra lệnh cho thiết bị nhớ để đặt bit kích hoạt nhằm cho phép thực thi điều khiển truy cập được tạo cấu hình hiện tại (nghĩa là thiết lập kênh an toàn giữa SOC và thiết bị nhớ theo khối cấu hình điều khiển truy cập đã cấu hình).

Trong khối 416, SOC có thể truy cập mảng bộ nhớ của thiết bị nhớ. Ví dụ, sau khi tạo cấu hình khối phần cứng điều khiển truy cập 130, SOC 140 có thể truy cập mảng ô RAM 138 để thực hiện các hoạt động đọc/ghi. Các lệnh mã hóa do SOC truyền và thiết bị nhớ nhận có thể bao gồm thông tin bổ sung bao gồm ID miền bảo mật để xác định thực thể bảo mật nào của SOC đang cố gắng truy cập vào các phần bộ nhớ cụ thể trong thiết bị nhớ. Bộ xử lý của SOC có thể đưa ra các hoạt động đóng/mở trang mà không có bảo vệ truy cập và có thể đưa ra các hoạt động đọc/ghi với bảo vệ truy cập.

Trong một số phương án, các lệnh đọc/ghi có thể được truyền tới thiết bị nhớ từ SOC theo các chuẩn bộ nhớ JEDEC. Ví dụ, việc triển khai các tiêu chuẩn JEDEC có thể bao gồm việc truyền các lệnh đọc/ghi qua bus JEDEC CMD và DATA, trong đó cmd opcode* chỉ rõ loại hoạt động (ví dụ: đọc, ghi hoặc nháy địa chỉ cột). Chuẩn JEDEC có thể được điều chỉnh, sửa đổi, sử dụng hoặc triển khai theo cách khác để bao gồm ID điều khiển truy cập** chỉ rõ miền bảo mật. Ví dụ, các bảng 5-7 minh họa lệnh đọc theo chuẩn JEDEC, trong đó Cas-3 là lệnh JEDEC bổ sung mới để bao gồm ID điều khiển truy cập chỉ rõ miền bảo mật. Đọc, Ghi, Cas-2, MRW-1 và MRW-2 (ghi thanh ghi chế độ) là các lệnh JEDEC hiện có.

Bảng 5

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Đọc		*cmd**	*cmd**	*cmd**					1
									2

Bảng 6

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2		cmd*	cmd*	cmd*					1
									2

Bảng 7

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-3		cmd*	cmd*	cmd*					1
					ID**	ID**	ID**	ID**	2

Kết quả của việc thực thi các lệnh mã hóa Đọc, Cas-2 và Cas-3 đối với quyền điều khiển truy cập của thiết bị nhớ là đọc 32 byte dữ liệu từ vị trí bộ nhớ tương ứng tới ID miền bảo mật được chỉ rõ trong lệnh Cas-3. Bảng 5-7 chỉ minh họa ví dụ cho phép SOC đọc 32 byte từ thiết bị nhớ. Lệnh ghi có thể được thực thi để ghi 32 byte vào vị trí bộ nhớ tương ứng với ID miền bảo mật theo cách tương tự như lệnh đọc (tức là thay thế "đọc" bằng "ghi" trong các lệnh JEDEC).

Trong một số phương án, các giao thức JEDEC có thể được sử dụng ở nhiều định dạng khác nhau tùy thuộc vào ứng dụng của hệ thống bao gồm SOC và thiết bị nhớ, sao cho thiết bị nhớ có thể được chuẩn hóa hoặc dành riêng cho ứng dụng. Ví dụ, bảng 8-11 minh họa loạt các lệnh để đọc 32 byte dữ liệu từ thiết bị nhớ.

Bảng 8

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Ghi		*cmd**	*cmd**	*cmd**					1
									2

Bảng 9

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2		cmd*	cmd*	cmd*					1
									2

Bảng 10

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Đọc		cmd*	cmd*	cmd*					1
									2

Bảng 11

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2		cmd*	cmd*	cmd*					1
									2

SOC có thể truyền lệnh tới bộ điều khiển truy cập của thiết bị nhớ chỉ rõ ID miền bảo mật. Ví dụ, SOC có thể truyền lệnh 32 byte bao gồm 1 byte dữ liệu để chỉ rõ ID miền bảo mật, và trong đó 31 byte còn lại bị bỏ qua, không liên quan hoặc chứa thông tin cho các mục đích khác ngoài việc xác định miền bảo mật. Lệnh này có thể được truyền cùng lúc, đồng thời hoặc về cơ bản là cùng thời điểm mà SOC thực thi lệnh Cas-2, sao cho điều khiển truy cập của thiết bị nhớ có thể liên kết lệnh Ghi và Cas-2 với ID miền bảo mật được chỉ rõ. Như vậy, điều khiển truy cập có thể được tạo cấu hình để theo dõi cụ thể việc nhận lệnh bao gồm ID miền bảo mật trên một giao diện bus khi nhận lệnh Cas-2 trên giao diện

bus khác. Ví dụ, như được mô tả thêm dựa vào Fig.3, khối phần cứng điều khiển truy cập 130 có thể nhận lệnh Cas-2 qua các kết nối 216d, 216 và có thể nhận ID miền bảo mật qua kết nối 304i. Bảng 8-11 chỉ minh họa một ví dụ cho phép SOC đọc 32 byte từ thiết bị nhớ. Lệnh ghi có thể được thực thi để ghi 32 byte vào vị trí bộ nhớ tương ứng với ID miền bảo mật theo cách tương tự như lệnh đọc (tức là thay thế "đọc" bằng "ghi" trong các lệnh JEDEC). Để giảm phí tổn, chế độ hoạt động bổ sung là khi khối phần cứng điều khiển truy cập đã nhận được ID miền bảo mật, các lệnh đọc hoặc ghi tiếp theo có thể nhận được thành công tương ứng với ID miền bảo mật gần đây nhất mà không cần gửi lại ID miền bảo mật mới. SOC 140 có thể tận dụng cơ hội này bằng cách gửi nhiều giao dịch đọc hoặc ghi tới RAM 122, tất cả đều thuộc cùng ID miền bảo mật, ví dụ: khối phần cứng điều khiển truy cập 130 sẽ giữ lại và áp dụng ID miền bảo mật hiện tại cho các giao dịch đọc hoặc ghi tiếp theo cho đến khi nhận được ID miền bảo mật mới. Do đó việc kết hợp các giao dịch với cùng ID có thể loại bỏ việc thiết lập ID miền bảo mật không cần thiết trong bảng 5,6 và 7.

Các bảng 12-14 minh họa định dạng ví dụ khác về triển khai các giao thức JEDEC để chỉ định (các) ID miền bảo mật.

Bảng 12

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
MRW-1		Cmd*	Cmd*	Cmd*				ID**	1
		Mode addr	Mode addr	Mode addr	Mode addr	Mode addr	Mode addr	Mode addr	2

Bảng 13

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
MRW-2		Cmd*	Cmd*	Cmd*				ID**	1
							ID**	ID**	2

Bảng 14

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Đọc		Cmd*	Cmd*	Cmd*					1
									2

Bảng 12-14 chỉ minh họa ví dụ cho phép SOC đọc 32 byte từ thiết bị nhớ. Lệnh ghi có thể được thực thi để ghi 32 byte vào vị trí bộ nhớ tương ứng với ID miền bảo mật theo cách tương tự như lệnh đọc (tức là thay thế "đọc" bằng "ghi" trong các lệnh JEDEC). Một lần nữa, ID miền bảo mật gần đây nhất có thể vẫn hoạt động và SOC 140 có thể gộp các giao dịch đọc hoặc ghi (phát hành liên tiếp) tương ứng với cùng ID miền bảo mật và giảm phí tổn tiêu tốn trong bảng 12 và 13.

Quay trở lại Fig.4, trong khối 418, SOC có thể triển khai chính sách điều khiển truy cập mới, chương trình, hoặc có thể đã cập nhật phân bổ bộ đệm bộ nhớ, và do đó có thể yêu cầu điều khiển truy cập thiết bị nhớ phải được tạo cấu hình lại dựa trên cập nhật phân bổ bộ nhớ đệm SOC. Khi xác định rằng phân bổ bộ đệm bộ nhớ SOC đã được tạo cấu hình lại hoặc cập nhật, các quy trình được mô tả trong khối 408-416 có thể được lặp lại để tạo cấu hình lại điều khiển truy cập của thiết bị nhớ. Việc triển khai SOC với bộ nhớ cập nhật không được phản ánh với điều khiển truy cập thiết bị nhớ sẽ dẫn đến lỗi và do đó yêu cầu thiết bị nhớ phải được tạo cấu hình lại để thích ứng với phân bổ bộ nhớ cập nhật cho trường hợp sử dụng phía SOC.

Fig.5 là sơ đồ khối thành phần minh họa ví dụ về hệ thống máy tính 500 bao gồm các đường giao dịch cấu hình và dữ liệu để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án. Tham chiếu đến các hình vẽ Fig.1-5, hệ thống 500 có thể bao gồm CPU 104, có thể bao gồm thực thể an toàn (ví dụ: cầu chì, vùng tin cậy) 502 và HLOS 504. Hệ thống 500 có thể bao gồm RAM 122, có thể bao gồm cấu trúc dữ liệu chính sách 506. Hệ thống có thể bao gồm các khối phần cứng và đường khác nhau để thực hiện các giao dịch chế độ cấu hình và giao dịch dữ liệu chế độ nhiệm vụ, trong đó cả hai bộ giao dịch được chuyển tiếp qua cùng giao diện PHY 124.

Các giao dịch chế độ cấu hình có thể được PHY 124 chuyển tiếp đến khối cấu hình điều khiển truy cập 132, trong đó đường 508 bao gồm các kết nối để chuyển tiếp địa chỉ và thông tin dữ liệu, cũng như các kết nối 514i để chuyển tiếp thông tin miền truy cập. Dữ liệu được chuyển tiếp qua đường 508 có thể bao gồm địa chỉ cơ sở, kích thước hoặc dải địa chỉ và ID miền bảo mật để tạo cấu hình khối cấu hình điều khiển truy cập 132 nhằm chuẩn bị cho các giao dịch dữ liệu chế độ nhiệm vụ. Các giao dịch cấu hình được chuyển tiếp qua đường 508 có thể được thực hiện như được mô tả với tham chiếu đến khối 414 của phương pháp 400 (Fig.4).

Các giao dịch dữ liệu chế độ nhiệm vụ có thể được PHY 124 chuyển tiếp đến khối thực thi chính sách 136, trong đó đường 510 bao gồm các kết nối để chuyển tiếp địa chỉ và thông tin dữ liệu, cũng như các kết nối 512i để chuyển tiếp thông tin miền truy cập. Thông tin được chuyển tiếp qua đường 510 có thể bao gồm thông tin địa chỉ và dữ liệu để đọc hoặc ghi vào vị trí cụ thể trong mảng ô RAM 138. Các giao dịch dữ liệu chế độ nhiệm vụ được chuyển tiếp qua đường 510 có thể được thực hiện như được mô tả với tham chiếu đến khối 416 của phương pháp 400 (Fig.4).

Fig.6 là sơ đồ dòng quy trình minh họa phương pháp 600 để theo dõi các vi phạm truy cập của thiết bị nhớ trong an toàn theo một số phương án. Tham chiếu đến các hình vẽ Fig.1-6, các hoạt động của phương pháp 600 có thể được thực hiện bởi bộ xử lý (ví dụ: CPU 104, NPU 308) của SOC (ví dụ: SOC 140) và khối phần cứng điều khiển truy cập (ví dụ: 130) của thiết bị nhớ ngoài (ví dụ: RAM 122).

Thứ tự của các hoạt động được thực hiện trong các khối 602-620 chỉ mang tính minh họa và các hoạt động của các khối 602-620 có thể được thực hiện theo thứ tự bất kỳ và một phần xảy ra đồng thời trong một số phương án. Trong một số phương án, phương pháp 600 có thể được thực hiện bởi bộ xử lý của thiết bị độc lập với, nhưng kết hợp với, thiết bị nhớ ngoài. Ví dụ, phương pháp 600 có thể được triển khai dưới dạng mođun phần mềm thực thi trong bộ xử lý của SOC hoặc trong phần cứng chuyên dụng trong SOC đưa ra các lệnh để cố gắng truy cập bộ nhớ của thiết bị nhớ ngoài và được tạo cấu hình theo cách khác để thực hiện các hành động và lưu trữ dữ liệu như mô tả.

Trong khối 602, điều khiển truy cập thiết bị nhớ có thể được tạo cấu hình và kích hoạt bởi khối phần cứng điều khiển truy cập. Điều này có thể được thực hiện như được mô tả với tham chiếu đến các khối 402-414 của phương pháp 400 (Fig.4), sao cho SOC tạo cấu hình điều khiển truy cập của khối phần cứng điều khiển truy cập của thiết bị nhớ để cho phép SOC đọc từ và/hoặc ghi vào bộ nhớ trong mảng ô thiết bị nhớ.

Trong khối 604, bộ xử lý SOC có thể gửi yêu cầu truy cập cùng với ID điều khiển truy cập tới bộ điều khiển bộ nhớ SOC. Ví dụ, như được mô tả dựa vào Fig.3, CPU 104 có thể tạo yêu cầu truy cập bộ nhớ để truy cập bộ nhớ cụ thể trong mảng ô RAM 138. Yêu cầu truy cập có thể được truyền bởi CPU 104 qua bus 118 tới bộ điều khiển bộ nhớ RAM 110. Yêu cầu truy cập có thể bao gồm ID điều khiển truy cập (ví dụ: ID miền bảo mật) để xác định rằng CPU 104 là nguồn của yêu cầu. Ví dụ khác, NPU 308 có thể truyền yêu cầu truy cập bao gồm ID điều khiển truy cập tới bộ điều khiển bộ nhớ RAM 110, trong đó ID điều khiển truy cập của NPU 308 khác với ID điều khiển truy cập của CPU 104.

Trong khối 606, bộ điều khiển bộ nhớ SOC có thể truyền lệnh đọc/ghi bao gồm ID điều khiển truy cập đến thiết bị nhớ để đáp lại việc nhận yêu cầu truy cập từ bộ xử lý SOC. Điều này có thể được thực hiện như được mô tả với tham chiếu đến khối 416 của phương pháp 400 (Fig.4).

Trong khối 608, khối phần cứng điều khiển truy cập có thể so sánh yêu cầu truy cập với cấu hình điều khiển truy cập. Ví dụ, như được mô tả dựa vào Fig.3, khối thực thi

chính sách 136 trong khối phần cứng điều khiển truy cập 130 có thể nhận yêu cầu truy cập từ PHY 124 và xác định xem yêu cầu truy cập bao gồm lệnh đọc/ghi có được cho phép hay không dựa trên cấu hình điều khiển truy cập được tạo cấu hình trong khối 602. Khối thực thi chính sách 136 trong khối phần cứng điều khiển truy cập 130 có thể phân tích yêu cầu truy cập để xác định địa chỉ cơ sở, dải địa chỉ và ID miền bảo mật, sau đó so sánh thông tin bộ nhớ và ID miền bảo mật với cấu hình điều khiển truy cập bộ nhớ (ví dụ: như được xác định bởi khối cấu hình điều khiển truy cập 132). Vị trí và phạm vi bộ nhớ xác định có thể được sử dụng để xác định thông tin bộ nhớ trong mảng ô nhớ RAM 138. ID bảo mật có thể xác định miền bảo mật của SOC đã khởi tạo yêu cầu truy cập, để miền bảo mật tương ứng với ID miền bảo mật đã yêu cầu thao tác đọc/ghi tại địa chỉ bộ nhớ và phạm vi đã xác định.

Trong khối xác định 610, khối phần cứng điều khiển truy cập 130 của thiết bị nhớ có thể xác định SOC có được cấp phép truy cập vào mảng ô nhớ của thiết bị nhớ hay không dựa trên yêu cầu truy cập và cấu hình điều khiển truy cập. Khối phần cứng điều khiển truy cập 130 có thể được tạo cấu hình để cho phép, ví dụ: triển khai khối thực thi chính sách 136) yêu cầu truy cập vào mảng ô nhớ dựa trên ID miền bảo mật cụ thể và các vị trí địa chỉ bộ nhớ và phạm vi tương ứng, trong khi từ chối các yêu cầu truy cập chỉ rõ ID miền bảo mật khác mà không được bao gồm trong cấu hình điều khiển truy cập bộ nhớ.

Ví dụ, Fig.7 minh họa bản đồ bộ nhớ hệ thống 700 để cung cấp điều khiển truy cập thiết bị nhớ trong an toàn theo một số phương án. Đối với ví dụ này, có thể giả định rằng CPU của SOC được gán ID miền bảo mật là 0 và NPU của cùng SOC đó được gán ID miền bảo mật là 1. Trong quá trình cấu hình điều khiển truy cập bộ nhớ, thiết bị nhớ có thể nhận được bản tin cấu hình bao gồm ID miền bảo mật là 0 và 1 tương ứng với CPU và NPU. Các bản tin cấu hình có thể bao gồm các vị trí địa chỉ bộ nhớ và phạm vi mà thiết bị nhớ sẽ cho phép truy cập dựa trên ID miền bảo mật tương ứng. Ví dụ, như được mô tả trong phương pháp 400 (Fig.4), thiết bị nhớ có thể đã nhận được các bản tin cấu hình để tạo cấu hình điều khiển truy cập nhằm cho phép hoạt động đọc/ghi được yêu cầu bởi NPU và CPU đối với dải địa chỉ bộ nhớ 704 và để cho phép các hoạt động đọc/ghi của CPU tới dải địa chỉ bộ nhớ 702 trong khi không cho phép các hoạt động đọc/ghi của NPU vào dải địa chỉ bộ nhớ 702. Ví dụ khác, điều khiển truy cập có thể được tạo cấu hình để cho phép các hoạt động đọc nhưng không cho phép các hoạt động ghi vào dải địa chỉ bộ nhớ 702 ngoại trừ CPU, để tất cả các miền bảo mật khác ngoài CPU bao gồm cả miền bảo mật NPU

có thể không ghi vào dải địa chỉ bộ nhớ 702. Do đó, nếu NPU thực hiện hoạt động 706 để yêu cầu ghi vào dải địa chỉ bộ nhớ 702, chính sách thực thi của thiết bị nhớ có thể kiểm tra yêu cầu có bao gồm ID miền bảo mật là 1 hay không, xác định rằng chỉ yêu cầu bao gồm ID miền bảo mật là 0 được cho phép ghi vào dải địa chỉ bộ nhớ 702 và có thể từ chối yêu cầu.

Quay trở lại Fig.6, để đáp lại việc xác định rằng vị trí và dải địa chỉ bộ nhớ và ID miền bảo mật của yêu cầu truy cập không được cho phép dựa trên cấu hình điều khiển truy cập (nghĩa là khối xác định 610 = "Không"), thì việc đọc/ghi của yêu cầu truy cập có thể không được thực hiện, lỗi có thể được ghi lại (ví dụ: thông qua khối hội chứng vi phạm truy cập 134) bao gồm thông tin yêu cầu truy cập và yêu cầu truy cập mới có thể được thực hiện trong khối 604.

Để đáp lại việc xác định rằng vị trí và dải địa chỉ bộ nhớ và ID miền bảo mật của yêu cầu truy cập được cho phép dựa trên cấu hình điều khiển truy cập (nghĩa là khối xác định 610 = "Có"), thì việc đọc/ghi của yêu cầu truy cập có thể được thực hiện ở khối 612. Khối 608, 610 và 612 có thể cho phép tiến hành nhiều giao dịch đọc và/hoặc ghi mà không phải gửi lại ID điều khiển truy cập trong khối 604 và 606. Nếu vậy, tất cả các giao dịch sẽ được xử lý như thuộc về ID miền bảo mật hiện tại đã được cung cấp trong khối 604 và 606 và mỗi giao dịch đọc hoặc ghi riêng lẻ sẽ được đánh giá dựa trên ID miền bảo mật hiện tại và được cấp phép hoặc từ chối truy cập một cách riêng lẻ.

Trong khối 614, bộ điều khiển bộ nhớ SOC chốt khóa dữ liệu phản hồi và phân tích tín hiệu chỉ báo lỗi. Ví dụ, như được mô tả dựa vào Fig.3, một hoặc nhiều lỗi có thể đã xảy ra khi yêu cầu truy cập gửi đến khối thực thi chính sách 136 hoặc trong hoạt động đọc/ghi vào mảng ô RAM 138. Hội chứng vi phạm truy cập có thể ghi lại bất kỳ lỗi nào, sau đó gửi thông tin lỗi tới SOC qua các kết nối 304e và 302e khi SOC gửi yêu cầu lệnh để truy xuất thông tin lỗi. Sau đó, bộ điều khiển bộ nhớ RAM 110 có thể chốt khóa dữ liệu phản hồi (ví dụ: tại kết nối 120d) sau khi hoạt động đọc/ghi được thực hiện, và có thể kiểm tra kết nối 302e để xác định xem có xuất hiện tín hiệu lỗi chỉ ra có bất kỳ lỗi xảy ra trong yêu cầu truy cập và/hoặc hoạt động đọc/ghi hay không.

Trong khối xác định 616, SOC có thể xác định xem có xảy ra lỗi hay không dựa trên tín hiệu lỗi nhận được từ thiết bị nhớ. Để đáp lại việc xác định rằng không có lỗi nào xảy ra (nghĩa là khối xác định 410 = "Không"), không có ngắt lỗi nào được báo cáo cho SOC và yêu cầu truy cập mới có thể được thực hiện theo khối 604.

Để đáp lại việc xác định rằng đã xảy ra lỗi (nghĩa là khối xác định 410 = "Có"), bộ điều khiển bộ nhớ SOC có thể yêu cầu thông tin lỗi từ thiết bị nhớ trong khối 618. Thông tin lỗi do hội chứng vi phạm truy cập bắt được có thể được thiết bị nhớ truyền tới SOC.

Trong khối 620, bộ điều khiển bộ nhớ SOC có thể lưu và lưu trữ cục bộ thông tin lỗi, sau đó kích hoạt ngắt đối tới bộ điều khiển chính SOC để thực hiện bất kỳ hoạt động cần thiết nào để ghi nhật ký và/hoặc khắc phục lỗi truy cập và/hoặc đọc/ghi.

Fig.8 là sơ đồ dòng quy trình minh họa phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án. Tham chiếu đến các hình vẽ Fig.1-8, các hoạt động của phương pháp 800 có thể được thực hiện bởi khối phần cứng điều khiển truy cập (ví dụ: 130) trong thiết bị nhớ (ví dụ: RAM 122) trong giao tiếp điện với bộ xử lý bên ngoài (ví dụ: CPU 104, NPU 308) của SOC (ví dụ: SOC 140).

Thứ tự của các hoạt động được thực hiện trong các khối 802-810 chỉ mang tính minh họa và các hoạt động của các khối 802-810 có thể được thực hiện theo thứ tự bất kỳ và một phần xảy ra đồng thời trong một số phương án. Trong một số phương án, phương pháp 800 có thể được thực hiện bởi khối phần cứng điều khiển truy cập trong thiết bị nhớ độc lập với, nhưng kết hợp với, bộ xử lý bên ngoài của SOC. Ví dụ, phương pháp 800 có thể được triển khai dưới dạng khối phần cứng điều khiển truy cập, có thể là phần cứng chuyên dụng trong thiết bị nhớ, thực thi cấu hình điều khiển truy cập bộ nhớ và các lệnh chế độ nhiệm vụ nhận được từ bộ xử lý của SOC.

Trong khối 802, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm bước nhận bản tin cấu hình từ SOC để tạo cấu hình điều khiển truy cập bộ nhớ của thiết bị nhớ. Trong một số phương án, bản tin cấu hình có thể bao gồm ID miền bảo mật cấu hình được sử dụng để tạo cấu hình điều khiển truy cập bằng khối phần cứng điều khiển truy cập của thiết bị nhớ. Trong một số phương án, bản tin cấu hình có thể là bản tin JEDEC được mã hóa bao gồm ID miền bảo mật cấu hình.

Trong khối 804, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm tạo cấu hình điều khiển truy cập bộ nhớ dựa trên bản tin cấu hình.

Trong khối 806, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm bước nhận bản tin yêu cầu truy cập từ SOC yêu cầu truy cập vào địa chỉ cơ sở của bộ nhớ và phạm vi truy cập bộ nhớ của mảng ô nhớ của thiết bị nhớ. Trong một số phương án, bản tin yêu cầu truy cập có thể bao gồm hoạt động đọc/ghi. Trong một số

phương án, bản tin yêu cầu truy cập có thể bao gồm ID miền bảo mật được yêu cầu được sử dụng để xác định miền bảo mật nào của SOC được yêu cầu hoạt động đọc/ghi. Trong một số phương án, bản tin yêu cầu truy cập có thể là bản tin JEDEC được mã hóa bao gồm ID miền bảo mật được yêu cầu.

Trong khối 808, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm so sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ đã được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được cho phép hay không.

Trong khối 810, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm cho phép hoạt động đọc/ghi để đáp lại việc xác định rằng bản tin yêu cầu truy cập được cho phép.

Fig.9 là sơ đồ dòng quy trình minh họa các hoạt động thay thế có thể được thực hiện bởi khối phần cứng điều khiển truy cập như là một phần của phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án. Tham chiếu đến các hình vẽ Fig.1-9, các hoạt động của phương pháp 900 có thể được thực hiện bởi khối phần cứng điều khiển truy cập (ví dụ: 130) trong thiết bị nhớ (ví dụ: RAM 122) trong giao tiếp điện với bộ xử lý bên ngoài (ví dụ: CPU 104, NPU 308) của SOC (ví dụ: SOC 140).

Sau khi thực hiện các hoạt động của khối 808 của phương pháp 800 (Fig.8), khối phần cứng điều khiển truy cập của thiết bị nhớ có thể thực hiện các hoạt động bao gồm xác định ID miền bảo mật cấu hình có khớp với ID miền bảo mật được yêu cầu trong khối 902 không. Điều này có thể được thực hiện như là một phần của các hoạt động được mô tả trong khối 808 của phương pháp 800 (Fig.8).

Trong khối 904, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm xác định bản tin yêu cầu truy cập được cho phép để đáp lại việc xác định ID miền bảo mật cấu hình khớp với ID miền bảo mật được yêu cầu.

Sau đó, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động của khối 810 của phương pháp 800 (Fig.8) như mô tả.

Fig.10 là sơ đồ dòng quy trình minh họa các hoạt động thay thế có thể được thực hiện bởi khối phần cứng điều khiển truy cập của thiết bị nhớ như là một phần của phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án. Tham chiếu đến các hình vẽ Fig.1-10, các hoạt động của phương pháp 1000 có thể được thực hiện bởi khối phần cứng điều khiển truy cập

(ví dụ: 130) của thiết bị nhớ (ví dụ: RAM 122) trong giao tiếp điện với bộ xử lý bên ngoài (ví dụ: CPU 104, NPU 308) của SOC (ví dụ: SOC 140).

Sau khi thực hiện các hoạt động của khối 808 của phương pháp 800 (Fig.8), khối phần cứng điều khiển truy cập của thiết bị nhớ có thể thực hiện các hoạt động bao gồm xác định rằng bản tin yêu cầu truy cập không được cho phép để đáp lại việc xác định rằng ID miền bảo mật cấu hình không khớp với ID miền bảo mật được yêu cầu trong khối 1002. Điều này có thể được thực hiện như là một phần của quy trình được mô tả trong khối 808 của phương pháp 800 (Fig.8).

Trong khối 1004, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm lưu trữ thông tin lỗi bao gồm địa chỉ cơ sở của bộ nhớ, phạm vi truy cập bộ nhớ và ID miền bảo mật được yêu cầu.

Trong khối 1006, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm truyền thông tin lỗi đến SOC.

Fig.11 là sơ đồ dòng quy trình minh họa các hoạt động thay thế có thể được thực hiện bởi khối phần cứng tin cậy của thiết bị nhớ như là một phần của phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án. Tham chiếu đến các hình vẽ Fig.1-11, các hoạt động của phương pháp 1100 có thể được thực hiện bởi khối phần cứng tin cậy (ví dụ: 125) của thiết bị nhớ (ví dụ: RAM 122) trong giao tiếp điện với bộ xử lý bên ngoài (ví dụ: CPU 104, NPU 308) của SOC (ví dụ: SOC 140).

Trong khối 1102, khối phần cứng tin cậy của thiết bị nhớ có thể thực hiện các hoạt động bao gồm bước nhận mật khẩu mở khóa từ SOC.

Trong khối 1104, khối phần cứng tin cậy có thể thực hiện các hoạt động bao gồm xác định xem mật khẩu mở khóa nhận được có khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận được lưu trữ trong thiết bị nhớ không.

Trong khối 1106, khối phần cứng tin cậy có thể thực hiện các hoạt động bao gồm mở khóa logic cổng thiết bị nhớ để cho phép khối phần cứng điều khiển truy cập nhận bản tin cấu hình để đáp lại việc xác định rằng mật khẩu mở khóa nhận được khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận.

Sau đó, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động của khối 802 của phương pháp 800 (Fig.8) như mô tả.

Fig.12 là sơ đồ dòng quy trình minh họa các hoạt động thay thế có thể được thực hiện bởi thiết bị nhớ như một phần của phương pháp 800 để cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án. Tham chiếu đến các hình vẽ Fig.1-12, các hoạt động của phương pháp 1200 có thể được thực hiện bởi khối phần cứng điều khiển truy cập (ví dụ: 130) của thiết bị nhớ (ví dụ: RAM 122) trong giao tiếp điện với bộ xử lý bên ngoài (ví dụ: CPU 104, NPU 308) của SOC (ví dụ: SOC 140).

Sau khi thực hiện các hoạt động của khối 804 của phương pháp 800 (Fig.8), khối phần cứng điều khiển truy cập của thiết bị nhớ có thể thực hiện các hoạt động bao gồm bước nhận, từ SOC, lệnh khóa được tạo cấu hình để thiết lập bit khóa trong thanh ghi của thiết bị nhớ trong khối 1202.

Trong khối 1204, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động bao gồm thiết lập bit khóa để ngăn thay đổi cấu hình đối với điều khiển truy cập bộ nhớ đã được tạo cấu hình.

Sau đó, khối phần cứng điều khiển truy cập có thể thực hiện các hoạt động của khối 806 của phương pháp 800 (Fig.8) như mô tả.

Các phương án khác nhau có thể được triển khai trong nhiều loại thiết bị điện toán, chẳng hạn như thiết bị điện toán đeo được. Fig.13 minh họa ví dụ về thiết bị điện toán đeo được ở dạng đồng hồ thông minh 1300 theo một số phương án. Đồng hồ thông minh 1300 có thể bao gồm bộ xử lý 1302 kết hợp với bộ nhớ trong 1304 và 1306. Bộ nhớ trong 1304, 1306 có thể là bộ nhớ khả biến hoặc bất khả biến và cũng có thể là bộ nhớ an toàn và/hoặc bộ nhớ được mã hóa, hoặc bộ nhớ không an toàn và/hoặc không được mã hóa hoặc bất kỳ sự kết hợp nào của chúng. Bộ xử lý 1302 cũng có thể được ghép nối với màn hình cảm ứng 1320, chẳng hạn như màn hình cảm ứng cảm ứng điện trở, màn hình cảm ứng cảm ứng điện dung cảm ứng hồng ngoại, hoặc tương tự. Ngoài ra, đồng hồ thông minh 1300 có thể có một hoặc nhiều ăngten 1308 để gửi và nhận bức xạ điện từ có thể được kết nối với một hoặc nhiều liên kết dữ liệu không dây 1312, chẳng hạn như một hoặc nhiều bộ thu phát Bluetooth®, bộ thu phát Peanut, bộ thu phát Wi-Fi, ANT+ bộ thu phát, v.v., có thể được ghép nối với bộ xử lý 1302. Đồng hồ thông minh 1300 cũng có thể bao gồm các nút vật lý ảo 1322 và 1310 để nhận đầu vào của người dùng cũng như cảm biến trượt 1316 để nhận đầu vào của người dùng.

Liên kết dữ liệu không dây 1312 và (các) bộ thu phát được kết nối có thể được sử dụng để ghép nối điện và giao tiếp với các thiết bị nhớ ngoài, chẳng hạn như RAM/NVRAM được ghép nối với bộ thu phát không dây đáp ứng. Ví dụ, như được mô tả thêm dựa vào Fig.3, đồng hồ thông minh 1300 có thể được ghép nối tạm thời với thiết bị nhớ ngoài (ví dụ: RAM 122), sao cho bộ xử lý (ví dụ: CPU 104) có thể tạo cấu hình điều khiển truy cập bộ nhớ (ví dụ: khối phần cứng điều khiển truy cập 130) để chuẩn bị đưa ra các lệnh để truy cập bộ nhớ (ví dụ: mảng ô RAM 138) của thiết bị nhớ.

Màn hình cảm ứng 1320 có thể được ghép nối với mođun giao diện màn hình cảm ứng được tạo cấu hình nhận tín hiệu từ màn hình cảm ứng 1320 cho biết các vị trí trên màn hình nơi đầu ngón tay hoặc bút stylus của người dùng chạm vào bề mặt và xuất ra đến bộ xử lý 1302 thông tin liên quan đến tọa độ của chạm vào các sự kiện. Hơn nữa, bộ xử lý 1302 có thể được tạo cấu hình với các lệnh có thể thực thi của bộ xử lý để tương quan hình ảnh được hiển thị trên màn hình cảm ứng 1320 với vị trí của các sự kiện chạm nhận được từ mođun giao diện màn hình cảm ứng để phát hiện khi người dùng đã tương tác với biểu tượng giao diện đồ họa, chẳng hạn như nút ảo.

Bộ xử lý 1302 có thể là bộ vi xử lý, máy vi tính hoặc chip hoặc nhiều chip đa xử lý có thể lập trình bất kỳ có thể được tạo cấu hình bằng các lệnh phần mềm (ứng dụng) để thực hiện nhiều chức năng khác nhau, bao gồm các chức năng của các phương án khác nhau. Trong các thiết bị, nhiều bộ xử lý có thể được cung cấp, chẳng hạn như một bộ xử lý dành riêng cho các chức năng truyền thông không dây và một bộ xử lý dành riêng để chạy các ứng dụng khác. Thông thường, các ứng dụng phần mềm có thể được lưu trữ trong bộ nhớ trong trước khi chúng được truy cập và tải vào bộ xử lý 1302. Bộ xử lý 1302 có thể bao gồm bộ nhớ trong đủ để lưu các lệnh phần mềm ứng dụng. Trong nhiều thiết bị, bộ nhớ trong có thể là bộ nhớ khả biến hoặc bất khả biến, chẳng hạn như bộ nhớ flash hoặc kết hợp cả hai. Đối với mục đích của mô tả này, việc nói chung đến bộ nhớ đề cập đến bộ nhớ mà bộ xử lý 1302 có thể truy cập bao gồm bộ nhớ trong hoặc bộ nhớ di động được đưa vào thiết bị di động và bộ nhớ trong chính bộ xử lý 1302.

Fig.14 là sơ đồ khối thành phần của ví dụ về thiết bị điện toán mạng 1400 có thể cung cấp truy cập thiết bị nhớ trong an toàn của thiết bị nhớ bằng hệ thống trên chip (SOC) theo một số phương án. Theo các FIG.1–14, thiết bị điện toán mạng 1400 có thể hoạt động như thành phần mạng của mạng truyền thông, chẳng hạn như trạm gốc. Thiết bị điện toán mạng 1400 có thể bao gồm bộ xử lý 1410 (ví dụ: CPU 104, NPU 308) được ghép nối với

bộ nhớ khả biến 1402 và bộ nhớ bất khả biến dung lượng lớn 1408 (ví dụ: RAM 122). Thiết bị điện toán mạng 1400 cũng có thể bao gồm thiết bị truy cập bộ nhớ ngoại vi chẳng hạn như ổ đĩa mềm, đĩa compac (CD) hoặc ổ đĩa viđeo số (DVD) 1406 được ghép nối với bộ xử lý 1410. Thiết bị điện toán mạng 1400 cũng có thể bao gồm các cổng truy cập mạng 1404 (hoặc các giao diện) được ghép nối với bộ xử lý 1410 để thiết lập các kết nối dữ liệu với mạng, chẳng hạn như mạng Internet hoặc mạng cục bộ được nối với các máy tính hệ thống và máy chủ khác. Thiết bị điện toán mạng 1400 có thể bao gồm một hoặc nhiều ăngten 1404 để gửi và nhận bức xạ điện từ có thể được kết nối với liên kết truyền thông không dây. Thiết bị điện toán mạng 1400 có thể bao gồm các cổng truy cập bổ sung, chẳng hạn như USB, Firewire, Thunderbolt, và những loại tương tự để ghép nối với thiết bị ngoại vi, bộ nhớ ngoài, hoặc các thiết bị khác.

Fig.15 là sơ đồ khối thành phần của thiết bị không dây ví dụ ở dạng điện thoại thông minh 1500 phù hợp để triển khai một sốphương án. Tham chiếu đến các hình vẽ Fig.1-15, điện thoại thông minh 1500 có thể bao gồm SOC thứ nhất 140 (chẳng hạn như SOC-CPU) được nối với SOC thứ hai 1502 (chẳng hạn như SOC có khả năng 5G). SOC thứ nhất và thứ hai 140, 1502 có thể được kết nối với bộ nhớ trong 1516 (ví dụ, SRAM 106), màn hình 1512 và với loa 1514. Ngoài ra, điện thoại thông minh 1500 có thể bao gồm ăngten 1504 để gửi và nhận bức xạ điện từ có thể được kết nối với liên kết dữ liệu không dây hoặc bộ thu phát điện thoại di động 1508 được ghép nối với một hoặc nhiều bộ xử lý trong SOC thứ nhất 140 hoặc thứ hai 1502. Ví dụ, ăngten 1504 có thể được sử dụng để kết nối điện và đưa ra các lệnh truy cập bộ nhớ chế độ nhiệm vụ và cấu hình cho thiết bị nhớ bên ngoài (ví dụ: RAM 122). Điện thoại thông minh 1500 thường cũng bao gồm các nút chọn menu hoặc chuyển mạch điều chỉnh 1520 để nhận các đầu vào người dùng.

Điện thoại thông minh điển hình 1500 cũng bao gồm mạch mã hóa/giải mã âm thanh (CODEC) 1510, giúp số hóa âm thanh nhận được từ micrô thành các gói dữ liệu phù hợp để truyền không dây và giải mã các gói dữ liệu âm thanh đã nhận để tạo ra tín hiệu tương tự được cung cấp cho loa để tạo ra âm thanh. Ngoài ra, một hoặc nhiều bộ xử lý trong SOC thứ nhất 140 và thứ hai 1502, bộ thu phát không dây 1508 và CODEC 1510 có thể bao gồm bộ xử lý tín hiệu kỹ thuật số (DSP) (không được thể hiện riêng).

Bộ xử lý của đồng hồ thông minh 1300, thiết bị điện toán mạng không dây 1400 và điện thoại thông minh 1500 có thể là bất kỳ bộ vi xử lý, máy vi tính hoặc chip hoặc các chip đa xử lý nào có thể được tạo cấu hình bằng các lệnh có thể thực thi của bộ xử lý để

thực hiện nhiều chức năng khác nhau, bao gồm các chức năng của các phương án khác nhau được mô tả ở đây. Trong các thiết bị không dây, nhiều bộ xử lý có thể được cung cấp, như một bộ xử lý trong SOC 1502 dành riêng cho các chức năng truyền thông không dây và một bộ xử lý trong SOC 140 dành riêng để chạy các ứng dụng khác. Thông thường, các ứng dụng phần mềm (ví dụ: chương trình tin cậy 102, 306) có thể được lưu trữ trong bộ nhớ 1506, 1516 trước khi chúng được truy cập và tải vào bộ xử lý. Bộ xử lý có thể bao gồm bộ nhớ trong đủ để lưu các lệnh phần mềm ứng dụng.

Khi được sử dụng trong sáng chế này, các thuật ngữ "thành phần", "mođun", "hệ thống" và các thuật ngữ tương tự nhằm mục đích bao gồm thực thể liên quan đến máy tính, như, nhưng không giới hạn ở, phần cứng, firmware, sự kết hợp của phần cứng và phần mềm, phần mềm, hoặc phần mềm đang thực thi, được tạo cấu hình để thực hiện các hoạt động hoặc chức năng cụ thể. Ví dụ, thành phần có thể là, nhưng không giới hạn ở, quy trình chạy trên bộ xử lý, bộ xử lý, đối tượng, tập tin thực thi được, chuỗi lệnh thực thi, chương trình, hoặc máy tính. Bằng cách minh họa, các ứng dụng chạy trên thiết bị không dây và thiết bị không dây có thể được gọi là thành phần. Một hoặc nhiều thành phần có thể nằm trong qui trình hoặc chuỗi lệnh thực thi và thành phần có thể được đặt cục bộ trên một bộ xử lý hoặc lõi hoặc được phân bố giữa hai hoặc nhiều bộ xử lý hoặc lõi. Ngoài ra, các thành phần này có thể thực thi từ các phương tiện có thể đọc được bằng máy tính bất biến khác nhau có các lệnh hoặc cấu trúc dữ liệu khác nhau được lưu trữ trên đó. Các thành phần có thể truyền thông nhờ các quy trình cục bộ hoặc từ xa, các cuộc gọi chức năng hoặc thủ tục, các tín hiệu điện tử, các gói dữ liệu, thủ tục ghi/đọc bộ nhớ, và các phương pháp truyền thông liên quan đến mạng, máy tính, bộ xử lý, hoặc quy trình đã biết khác.

Các phương án khác nhau được minh họa và mô tả chỉ được cung cấp làm ví dụ để minh họa các đặc điểm khác nhau của các yêu cầu bảo. Tuy nhiên, các đặc điểm được thể hiện và mô tả liên quan đến bất kỳ phương án đã cho nào không nhất thiết bị giới hạn ở phương án liên quan đó và có thể được sử dụng hoặc kết hợp với các phương án khác được chỉ ra và được mô tả. Hơn nữa, các yêu cầu bảo hộ không nhằm giới hạn bởi bất kỳ một phương án ví dụ nào. Ví dụ, một hoặc nhiều hoạt động của các phương pháp được tiết lộ ở đây có thể được thay thế hoặc kết hợp với một hoặc nhiều hoạt động của các phương pháp được tiết lộ ở đây.

Các mô tả phương pháp nêu trên và lưu đồ được cung cấp chỉ đơn thuần là các ví dụ minh họa và không nhằm yêu cầu hoặc ngụ ý rằng các bước của một số phương án có

thể được thực hiện theo thứ tự được trình bày. Những người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể hiểu rõ rằng thứ tự các bước trong các phương án ở trên có thể được thực hiện theo bất kỳ thứ tự nào. Các từ như "sau đó", "tiếp theo", v.v. không nhằm giới hạn thứ tự của các khối; những từ này chỉ được sử dụng để hướng dẫn người đọc thông qua mô tả của các phương pháp. Hơn nữa, bất kỳ sự viện dẫn nào để đề cập đến các phần tử ở dạng số ít, ví dụ, bằng cách sử dụng các mạo từ số ít không được hiểu là giới hạn phần này ở dạng số ít.

Như được sử dụng ở đây, cụm từ đề cập đến "ít nhất một trong số" danh sách các mục đề cập đến sự kết hợp bất kỳ của các mục đó, bao gồm cả các thành viên đơn lẻ. Ví dụ, "ít nhất một trong số: a, b, hoặc c" được dùng để bao hàm: a, b, c, a-b, a-c, b-c và a-b-c.

Các khối lôgic minh họa, mođun, mạch và các bước thuật toán khác nhau được mô tả liên quan đến các phương án được bộc lộ ở đây có thể được triển khai dưới dạng phần cứng điện tử, phần mềm máy tính hoặc kết hợp của cả hai. Để minh họa rõ ràng khả năng thay thế cho nhau của phần cứng và phần mềm, các thành phần, khối, mođun, mạch và các bước minh họa khác nhau đã được mô tả chung ở trên về chức năng của chúng. Việc chức năng đó được triển khai dưới dạng phần cứng hay phần mềm phụ thuộc vào các ràng buộc thiết kế và ứng dụng cụ thể được áp đặt trên toàn bộ hệ thống. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng có thể triển khai chức năng được mô tả theo nhiều cách khác nhau cho từng ứng dụng cụ thể, nhưng các quyết định theo phương án như vậy không nên được hiểu là gây ra sự khác biệt với phạm vi của các yêu cầu bảo hộ.

Phần cứng và thiết bị xử lý dữ liệu được dùng để thực hiện các logic, khối logic, mođun và mạch minh họa được mô tả liên quan đến các khía cạnh được trình bày ở đây có thể được thực thi hoặc thực hiện với bộ xử lý một hoặc nhiều chip, bộ xử lý tín hiệu số (digital signal processor - DSP), mạch tích hợp chuyên dụng (application specific integrated circuit - ASIC), mảng cổng lập trình được theo trường (field programmable gate array - FPGA) hoặc thiết bị logic lập trình được khác, cổng rời rạc hoặc logic bán dẫn , các thành phần phần cứng rời rạc hoặc kết hợp bất kỳ của chúng được thiết kế để thực hiện các chức năng được mô tả trong sáng chế này. Bộ xử lý đa dụng có thể là bộ vi xử lý, hoặc, bất kỳ bộ xử lý, bộ điều khiển, bộ vi điều khiển, hoặc máy trạng thái thông thường. Bộ xử lý cũng có thể được triển khai dưới dạng kết hợp, ví dụ như, kết hợp giữa DSP và bộ vi xử lý, nhiều bộ vi xử lý, một hoặc nhiều bộ vi xử lý kết hợp với lõi DSP hoặc cấu hình như

vậy khác bất kỳ. Trong một số phương án triển khai, các quy trình và phương pháp cụ thể có thể được thực hiện bằng mạch điện cho chức năng nhất định.

Theo một hoặc nhiều khía cạnh, các chức năng được mô tả có thể được thực hiện trong phần cứng, mạch điện tử kỹ thuật số, phần mềm máy tính, firmware, bao gồm các cấu trúc được bộc lộ trong bản mô tả này và các tương đương về cấu trúc của chúng, hoặc trong bất kỳ sự kết hợp nào của chúng. Các phương án của đối tượng được mô tả trong đặc điểm kỹ thuật này cũng có thể được triển khai dưới dạng một hoặc nhiều chương trình máy tính, tức là một hoặc nhiều mođun của hướng dẫn chương trình máy tính, được mã hóa trên phương tiện lưu trữ máy tính để thực thi hoặc kiểm soát hoạt động của thiết bị xử lý dữ liệu.

Mã chương trình máy tính hoặc "mã chương trình" để thực thi trên bộ xử lý có thể lập trình nhằm thực hiện các hoạt động của các phương án khác nhau có thể được viết bằng ngôn ngữ lập trình cấp cao như C, C++, C#, Smalltalk, Java, JavaScript, Visual Basic, Ngôn ngữ truy vấn có cấu trúc (ví dụ: Transact-SQL), Perl hoặc bằng nhiều ngôn ngữ lập trình khác. Mã chương trình hoặc các chương trình được lưu trữ trên phương tiện lưu trữ đọc được bằng máy tính như được dùng trong sáng chế này có thể chỉ mã ngôn ngữ máy (như mã đối tượng) mà bộ xử lý có thể hiểu được định dạng của nó.

Nếu được thực hiện bằng phần mềm, các chức năng có thể được lưu trữ trên hoặc truyền dưới dạng một hoặc nhiều lệnh hoặc mã trên phương tiện đọc được bằng máy tính. Các quy trình của phương pháp hoặc thuật toán được mô tả ở đây có thể được triển khai trong mođun phần mềm thực thi được bằng bộ xử lý mà có thể nằm trên phương tiện đọc được bằng máy tính. Phương tiện đọc được bằng máy tính bao gồm cả phương tiện lưu trữ máy tính và phương tiện truyền thông bao gồm bất kỳ phương tiện nào có thể được kích hoạt để truyền chương trình máy tính từ nơi này sang nơi khác. Phương tiện lưu trữ có thể là bất kỳ phương tiện sẵn có nào có thể được truy cập bởi máy tính. Ví dụ, và không giới hạn, phương tiện đọc được bằng máy tính như vậy có thể bao gồm RAM, ROM, EEPROM, CD-ROM hoặc thiết bị lưu trữ đĩa quang khác, thiết bị lưu trữ đĩa từ hoặc các thiết bị lưu trữ từ tính khác, hoặc phương tiện khác bất kỳ có thể được dùng để lưu trữ mã chương trình mong muốn là lệnh hoặc cấu trúc dữ liệu và có thể được máy tính truy nhập. Ngoài ra, bất kỳ kết nối nào cũng có thể được gọi là phương tiện đọc được bằng máy tính. Đĩa từ và đĩa quang, như được sử dụng ở đây, bao gồm đĩa compac (compact disc - CD), đĩa laze, đĩa quang, đĩa số đa năng (DVD - Digital Versatile Disc), đĩa mềm và đĩa bluray, trong đó

đĩa từ thường tái tạo dữ liệu bằng phương pháp từ tính, còn đĩa quang thường tái tạo dữ liệu bằng phương pháp quang học sử dụng laze. Sự kết hợp của các loại trên cũng được bao gồm trong phạm vi của phương tiện đọc được bằng máy tính. Ngoài ra, các hoạt động của phương pháp hoặc thuật toán có thể nằm trong một hoặc tổ hợp hoặc tập hợp mã và lệnh bất kỳ trên phương tiện đọc được bằng máy và phương tiện đọc được bằng máy tính, có thể được tích hợp vào sản phẩm chương trình máy tính.

Có nhiều cải biến đối với các phương án của sáng chế sẽ được người có hiểu biết trung bình trong lĩnh vực kỹ thuật này tìm ra một cách dễ dàng, và các nguyên lý chung đã nêu ra trong sáng chế có thể áp dụng cho những phương án khác mà không bị coi là vượt ra ngoài phạm vi của sáng chế. Do đó, yêu cầu bảo hộ không dự định bị giới hạn ở các phương án được thể hiện ở đây mà phải được hiểu có phạm vi rộng nhất phù hợp với sáng chế này, các nguyên tắc và các tính năng mới được tiết lộ ở đây.

YÊU CẦU BẢO HỘ

1. Phương pháp chỉ báo phản hồi về việc chấp nhận truy cập/vi phạm cho hệ thống trên chip, system on chip – SOC, như là một phần của chuỗi giao dịch đọc/ghi của thiết bị nhớ, được đặc trưng bởi việc bao gồm các bước:

nhận mật khẩu mở khóa từ SOC;

xác định xem mật khẩu mở khóa nhận được có khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận được lưu trữ trong thiết bị nhớ hay không; và

mở khóa logic cổng thiết bị nhớ để cho phép điều khiển truy cập bộ nhớ nhận bản tin cấu hình để đáp lại việc xác định rằng mật khẩu mở khóa nhận được khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận;

nhận bản tin cấu hình từ SOC để tạo cấu hình điều khiển truy cập bộ nhớ của thiết bị nhớ;

tạo cấu hình điều khiển truy cập bộ nhớ dựa trên bản tin cấu hình;

nhận bản tin yêu cầu truy cập từ SOC yêu cầu truy cập vào địa chỉ cơ sở của bộ nhớ và phạm vi truy cập bộ nhớ của mảng ô nhớ của thiết bị nhớ, trong đó bản tin yêu cầu truy cập bao gồm hoạt động đọc/ghi;

so sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ đã được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được cho phép hay không; và

thực hiện hoạt động đọc/ghi để đáp lại việc xác định rằng bản tin yêu cầu truy cập được cho phép.

2. Phương pháp theo điểm 1, khác biệt ở chỗ:

bản tin cấu hình bao gồm ID miền bảo mật cấu hình; và

bản tin yêu cầu truy cập bao gồm ID miền bảo mật được yêu cầu.

3. Phương pháp theo điểm 2, khác biệt ở chỗ việc so sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ đã được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được cho phép hay không bao gồm:

xác định xem ID miền bảo mật cấu hình có khớp với ID miền bảo mật được yêu cầu hay không; và

để đáp lại việc xác định rằng ID miền bảo mật cấu hình khớp với ID miền bảo mật được yêu cầu:

xác định rằng bản tin yêu cầu truy cập được cho phép; và

truyền thông báo đến SOC cho biết rằng bản tin yêu cầu truy cập được cho phép.

4. Phương pháp theo điểm 3, còn được đặc trưng bởi việc bao gồm các bước:

để đáp lại việc xác định rằng ID miền bảo mật cấu hình không khớp với ID miền bảo mật được yêu cầu:

xác định rằng bản tin yêu cầu truy cập là không được cho phép;

lưu trữ thông tin lỗi bao gồm địa chỉ cơ sở của bộ nhớ, phạm vi truy cập bộ nhớ, và ID miền bảo mật được yêu cầu;

truyền thông báo đến SOC cho biết rằng bản tin yêu cầu truy cập không được cho phép; và

truyền thông tin lỗi đến SOC để đáp lại việc nhận được yêu cầu ngắt do lỗi từ SOC.

5. Phương pháp theo điểm 2, khác biệt ở chỗ:

bản tin cấu hình là bản tin JEDEC được mã hóa bao gồm ID miền bảo mật cấu hình; và

bản tin yêu cầu truy cập là bản tin JEDEC được mã hóa bao gồm ID miền bảo mật được yêu cầu.

6. Phương pháp theo điểm 1, còn được đặc trưng bởi việc bao gồm các bước:

nhận, từ SOC, lệnh khóa được tạo cấu hình để thiết lập bit khóa trong thanh ghi của thiết bị nhớ; và

thiết lập bit khóa để ngăn thay đổi cấu hình đối với điều khiển truy cập bộ nhớ đã được tạo cấu hình.

7. Thiết bị nhớ, được đặc trưng bởi việc bao gồm:

mảng ô nhớ;

logic cổng thiết bị nhớ;

khối phần cứng tin cậy, trong đó khối phần cứng tin cậy được tạo cấu hình để thực hiện các hoạt động còn bao gồm:

nhận mật khẩu mở khóa từ SOC;

xác định xem mật khẩu mở khóa nhận được có khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận được lưu trữ trong thiết bị nhớ hay không; và

mở khóa logic cổng thiết bị nhớ để cho phép điều khiển truy cập bộ nhớ nhận bản tin cấu hình để đáp lại việc xác định rằng mật khẩu mở khóa nhận được khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận; và

trong đó khối phần cứng điều khiển truy cập được tạo cấu hình để thực hiện các hoạt động bao gồm:

nhận bản tin cấu hình từ SOC để tạo cấu hình điều khiển truy cập bộ nhớ của thiết bị nhớ;

tạo cấu hình điều khiển truy cập bộ nhớ dựa trên bản tin cấu hình;

nhận bản tin yêu cầu truy cập từ SOC yêu cầu truy cập vào địa chỉ cơ sở của bộ nhớ và phạm vi truy cập bộ nhớ của mảng ô nhớ, trong đó bản tin yêu cầu truy cập bao gồm hoạt động đọc/ghi;

so sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ đã được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được cho phép hay không; và

thực hiện hoạt động đọc/ghi để đáp lại việc xác định rằng bản tin yêu cầu truy cập được cho phép.

8. Thiết bị nhớ theo điểm 7, khác biệt ở chỗ khối phần cứng điều khiển truy cập được tạo cấu hình để thực hiện các hoạt động sao cho:

việc nhận bản tin cấu hình từ SOC bao gồm bước nhận bản tin cấu hình gồm ID miền bảo mật cấu hình; và

việc nhận bản tin yêu cầu truy cập từ SOC bao gồm bước nhận bản tin yêu cầu truy cập gồm ID miền bảo mật được yêu cầu.

9. Thiết bị nhớ theo điểm 8, khác biệt ở chỗ khối phần cứng điều khiển truy cập được tạo cấu hình để thực hiện các hoạt động sao cho việc so sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ đã được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được cho phép hay không bao gồm:

xác định xem ID miền bảo mật cấu hình có khớp với ID miền bảo mật được yêu cầu hay không; và

để đáp lại việc xác định rằng ID miền bảo mật cấu hình khớp với ID miền bảo mật được yêu cầu:

xác định rằng bản tin yêu cầu truy cập được cho phép; và

truyền thông báo đến SOC cho biết rằng bản tin yêu cầu truy cập được cho phép.

10. Thiết bị nhớ theo điểm 9, khác biệt ở chỗ khối phần cứng điều khiển truy cập được tạo cấu hình để thực hiện các hoạt động còn bao gồm:

để đáp lại việc xác định rằng ID miền bảo mật cấu hình không khớp với ID miền bảo mật được yêu cầu:

xác định rằng bản tin yêu cầu truy cập là không được cho phép;

lưu trữ thông tin lỗi bao gồm địa chỉ cơ sở của bộ nhớ, phạm vi truy cập bộ nhớ và ID miền bảo mật được yêu cầu;

truyền thông báo đến SOC cho biết rằng bản tin yêu cầu truy cập không được cho phép; và

truyền thông tin lỗi đến SOC đáp lại việc nhận được yêu cầu ngắt do lỗi từ SOC.

11. Thiết bị nhớ theo điểm 8, khác biệt ở chỗ khối phần cứng điều khiển truy cập được tạo cấu hình để thực hiện các hoạt động sao cho:

việc nhận bản tin cấu hình từ SOC bao gồm bước nhận bản tin JEDEC được mã hóa gồm ID miền bảo mật cấu hình; và

việc nhận bản tin yêu cầu truy cập từ SOC bao gồm bước nhận bản tin JEDEC được mã hóa gồm ID miền bảo mật được yêu cầu.

12. Thiết bị nhớ theo điểm 7, khác biệt ở chỗ khối phần cứng tin cậy được tạo cấu hình để thực hiện các hoạt động còn bao gồm:

nhận, từ SOC, lệnh khóa được tạo cấu hình để thiết lập bit khóa trong thanh ghi của thiết bị nhớ; và

thiết lập bit khóa để ngăn thay đổi cấu hình đối với điều khiển truy cập bộ nhớ đã được tạo cấu hình.

13. Thiết bị nhớ theo điểm 7, khác biệt ở chỗ khối phần cứng tin cậy bao gồm:

bộ nhớ cầu chì được tạo cấu hình để lưu trữ tập hợp các mật khẩu được chấp nhận;

cổng chấp nhận bao gồm logic cổng thiết bị nhớ; và

khối logic được ghép nối với bộ nhớ cầu chì và cổng chấp nhận và được tạo cấu hình để:

xác định xem mật khẩu mở khóa nhận được có khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận được lưu trữ trong bộ nhớ cầu chì hay không; và

báo hiệu cho cổng chấp nhận để mở khóa logic cổng thiết bị nhớ để đáp lại việc xác định rằng mật khẩu mở khóa nhận được khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận được lưu trữ trong bộ nhớ cầu chì.

14. Thiết bị nhớ theo điểm 7, khác biệt ở chỗ khối phần cứng điều khiển truy cập bao gồm:

khối cấu hình điều khiển truy cập;

hội chứng vi phạm truy cập; và

khối thực thi chính sách.

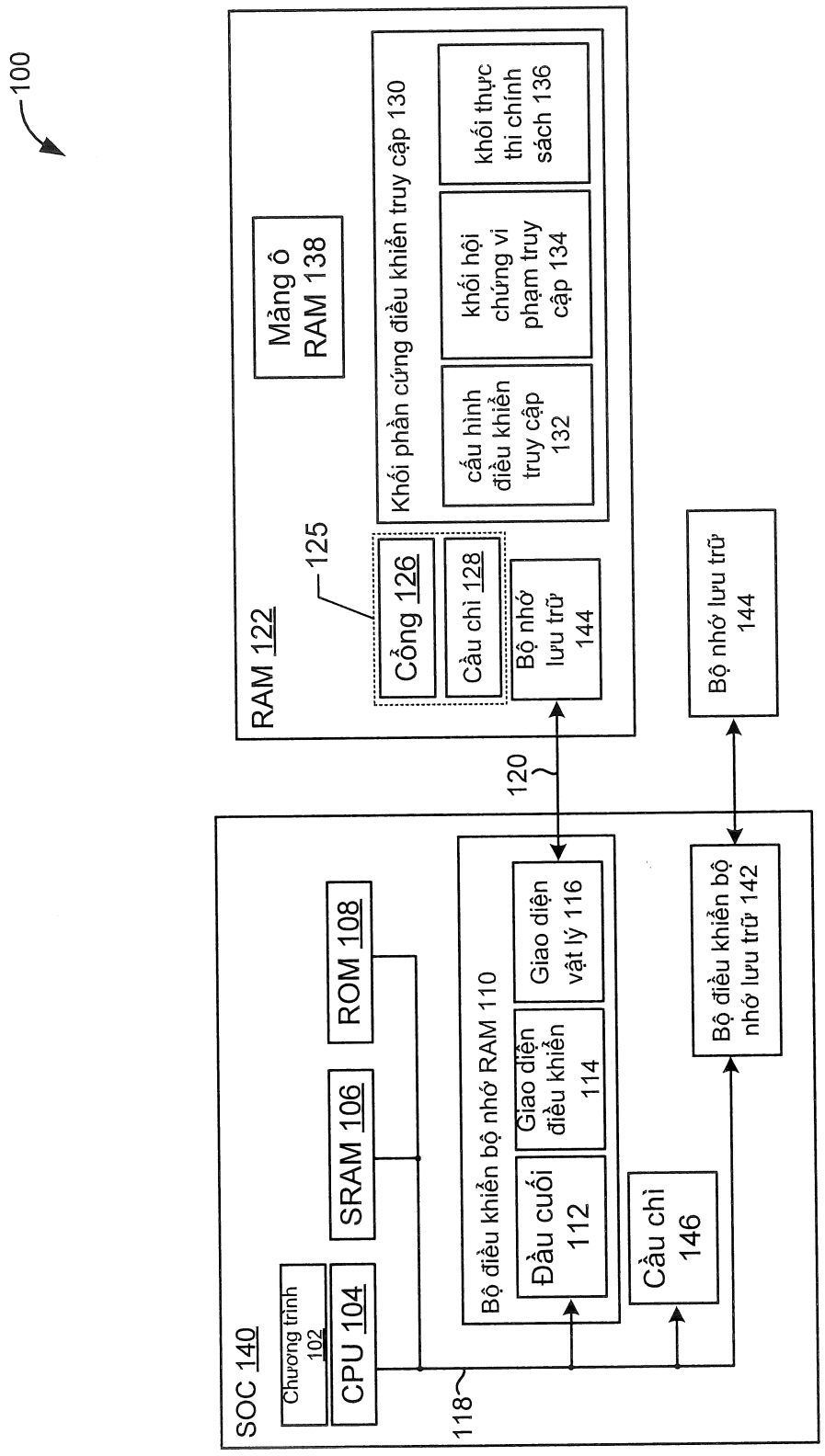
100
SOC 140
Chương trình 102
CPU 104
SRAM 106
ROM 108
118
Bộ điều khiển bộ nhớ RAM 110
Đầu cuối 112
Giao diện điều khiển 114
Giao diện vật lý 116
Cầu chì 146
Bộ điều khiển bộ nhớ lưu trữ 142
120
RAM 122
125
Cổng 126
Cầu chì 128
Bộ nhớ lưu trữ 144
Khối phần cứng điều khiển truy cập 130
cấu hình điều khiển truy cập 132
khối hội chứng vi phạm truy cập 134
khối thực thi chính sách 136
Mảng ô RAM 138
Bộ nhớ lưu trữ 144

FIG. 1

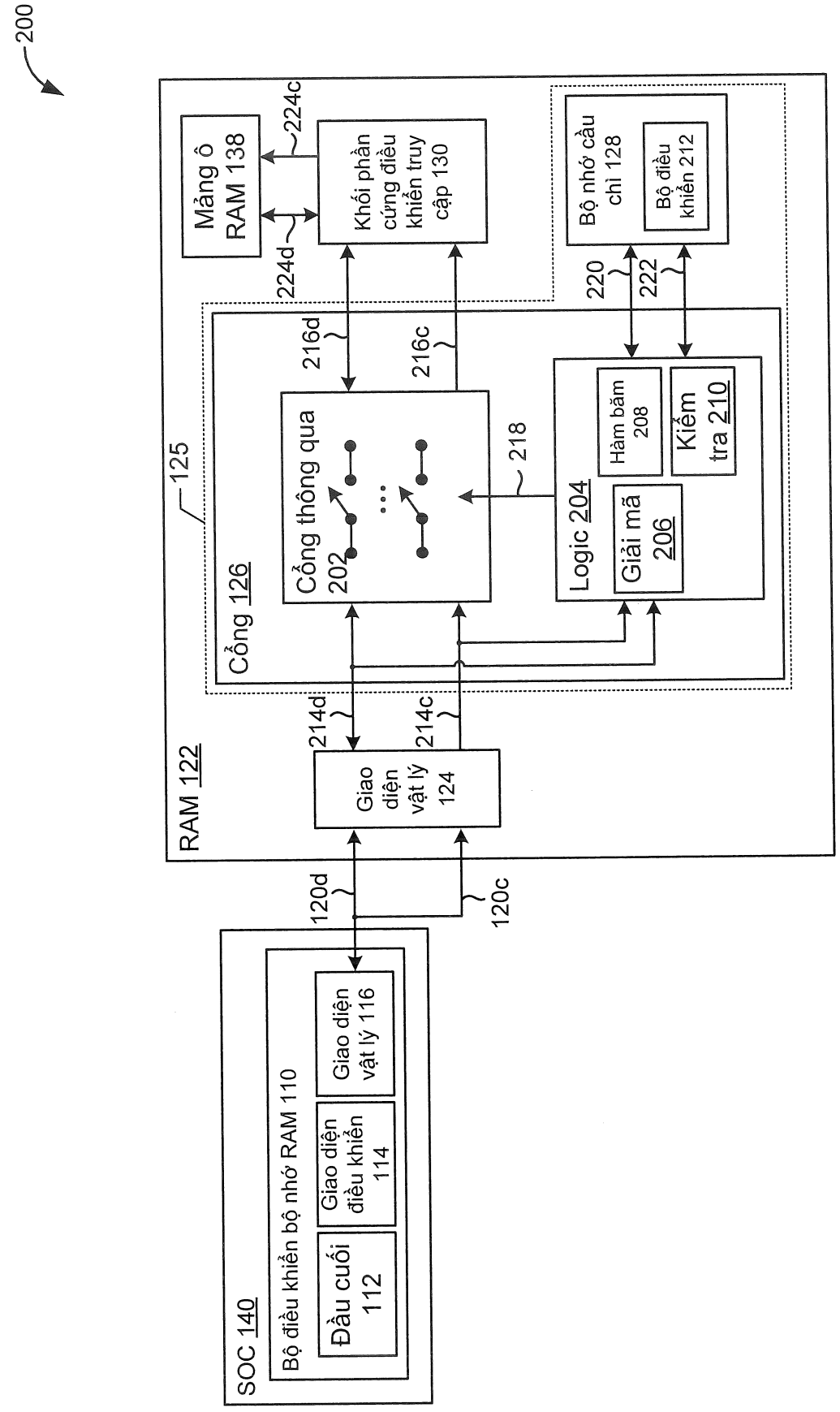
200
SOC 140
Bộ điều khiển bộ nhớ RAM 110
Đầu cuối 112
Giao diện điều khiển 114
Giao diện vật lý 116
120d
120c
RAM 122
Giao diện vật lý 124
214d
214c
125
Cổng 126
Cổng thông qua 202
216d
216c
218
Logic 204
Giải mã 206
Hàm băm 208
Kiểm tra 210
Bộ nhớ cầu chì 128
Bộ điều khiển 212
220
222
Mảng ô RAM 138
Khối phần cứng điều khiển truy cập 130
224c
224d

FIG. 2

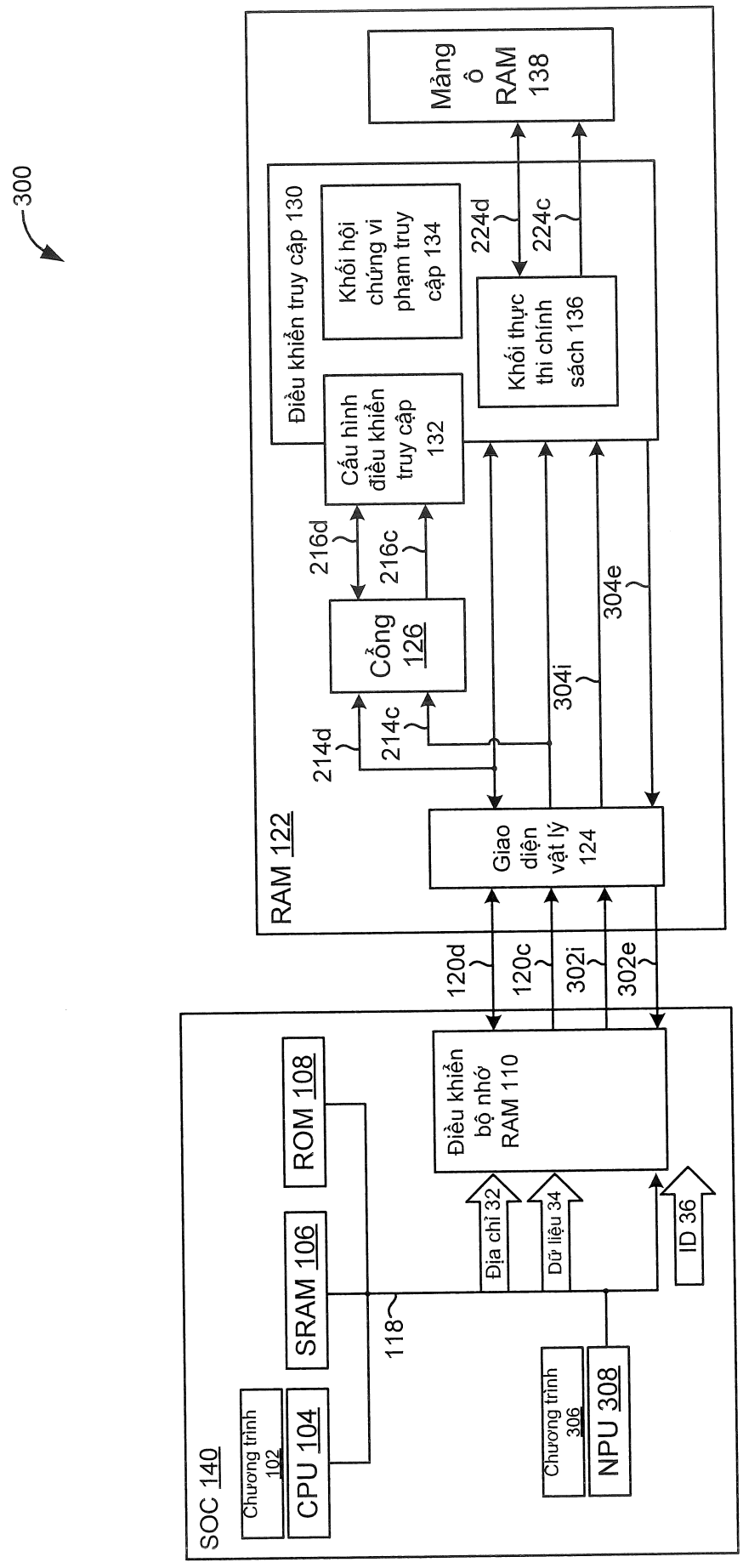
300
SOC 140
Chương trình 102
CPU 104
SRAM 106
ROM 108
118
Địa chỉ 32
Dữ liệu 34
ID 36
Điều khiển bộ nhớ RAM 110
Chương trình 306
NPU 308
120d
120c
302i
302e
RAM 122
Giao diện vật lý 124
214d
214c
Cổng 126
216d
216c
Điều khiển truy cập 130
Cấu hình điều khiển truy cập 132
Khối hội chứng vi phạm truy cập 134
Khối thực thi chính sách 136
304i
304e
224d
224c
Mảng ô RAM 138

FIG. 3

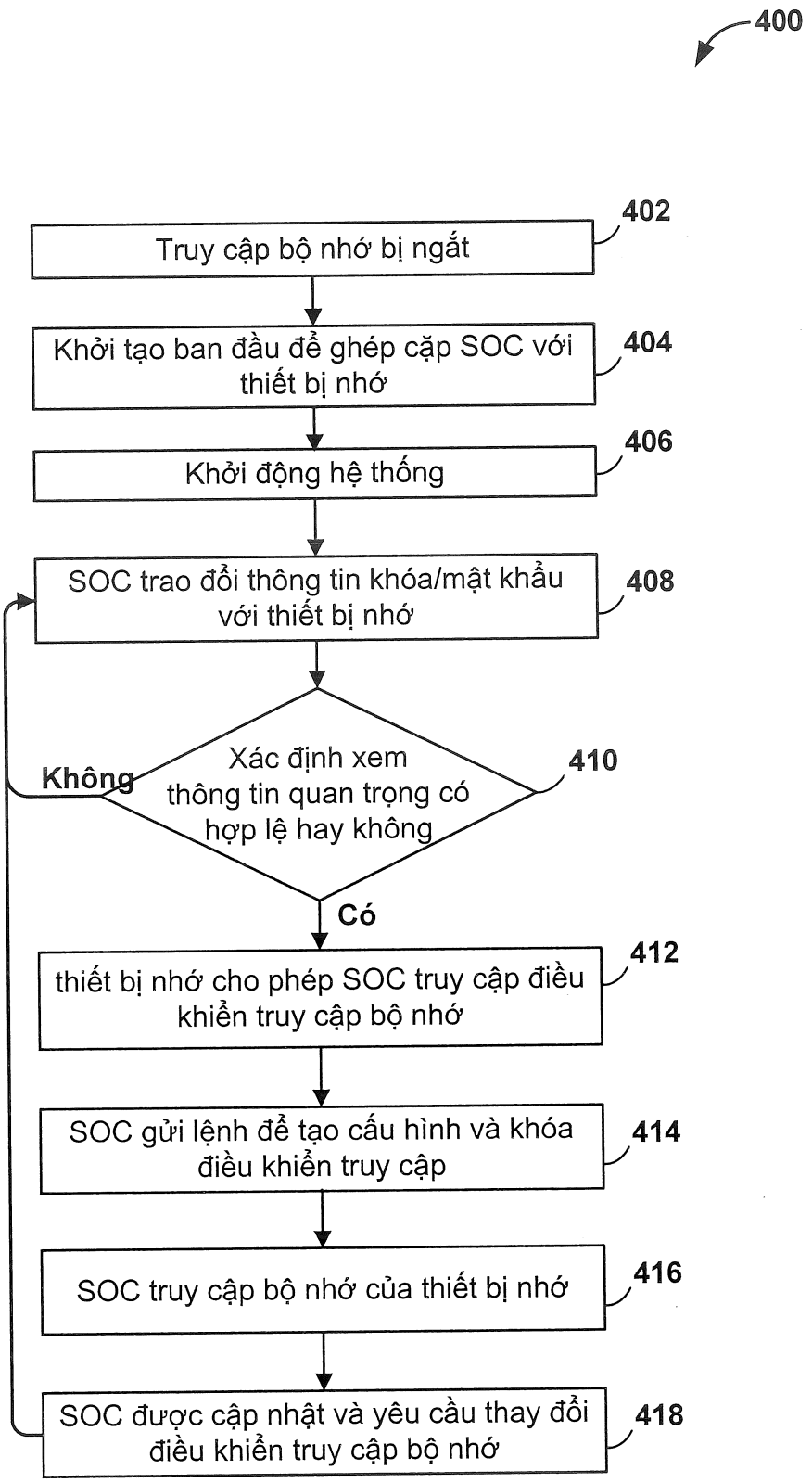
400
402
Truy cập bộ nhớ bị ngắt
404
Khởi tạo ban đầu để ghép cặp SOC với thiết bị nhớ
406
Khởi động hệ thống
408
SOC trao đổi thông tin khóa/mật khẩu với thiết bị nhớ
410
Xác định xem thông tin quan trọng có hợp lệ hay không
Không
Có
412
thiết bị nhớ cho phép SOC truy cập điều khiển truy cập bộ nhớ
414
SOC gửi lệnh để tạo cấu hình và khóa điều khiển truy cập
416
SOC truy cập bộ nhớ của thiết bị nhớ
418
SOC được cập nhật và yêu cầu thay đổi điều khiển truy cập bộ nhớ

FIG. 4

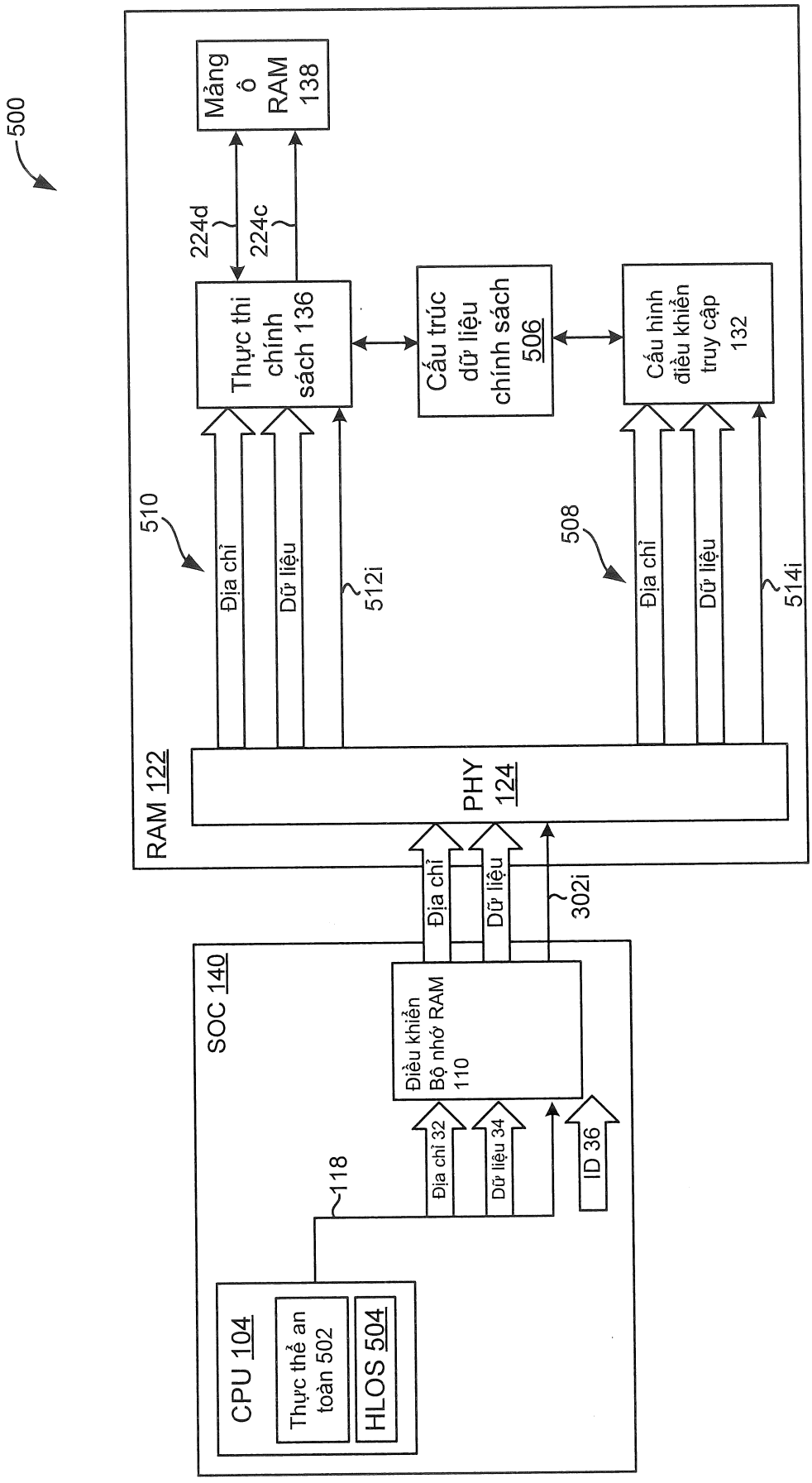
500
Mảng ô RAM 138
224d
224c
Thực thi chính sách 136
Cấu trúc dữ liệu chính sách 506
Cấu hình điều khiển truy cập 132
510
Địa chỉ
Dữ liệu
512i
508
Địa chỉ
Dữ liệu
514i
RAM 122
PHY 124
Địa chỉ
Dữ liệu
302i
SOC 140
Điều khiển Bộ nhớ RAM 110
Địa chỉ 32
Dữ liệu 34
ID 36
118
CPU 104
Thực thể an toàn 502
HLOS 504

FIG. 5

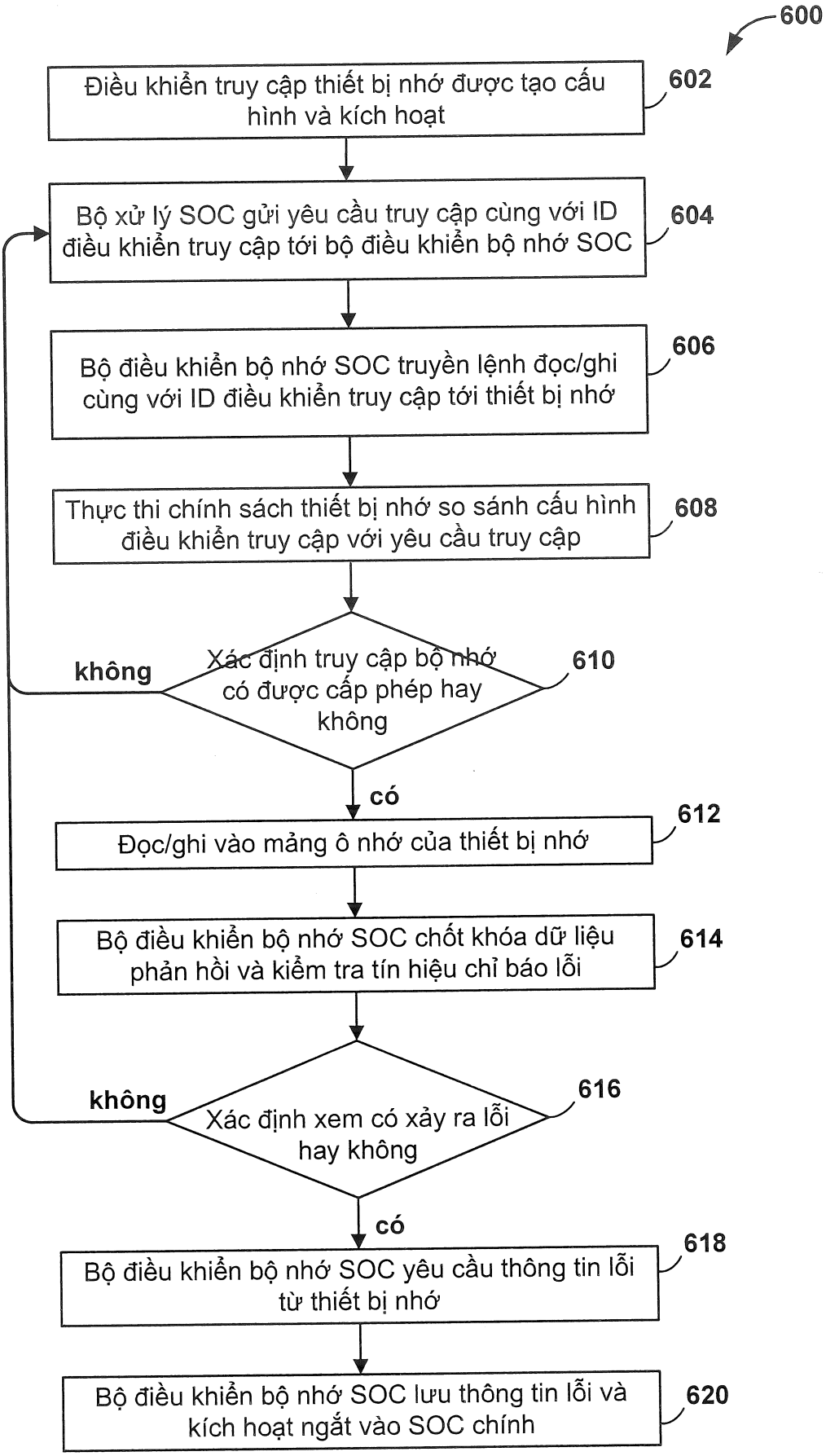
600
Điều khiển truy cập thiết bị nhớ được tạo cấu hình và kích hoạt
602
Bộ xử lý SOC gửi yêu cầu truy cập cùng với ID điều khiển truy cập tới bộ điều khiển bộ nhớ SOC
604
Bộ điều khiển bộ nhớ SOC truyền lệnh đọc/ghi cùng với ID điều khiển truy cập tới thiết bị nhớ
606
Thực thi chính sách thiết bị nhớ so sánh cấu hình điều khiển truy cập với yêu cầu truy cập
608
Xác định truy cập bộ nhớ có được cấp phép hay không
610
không
có
Đọc/ghi vào mảng ô nhớ của thiết bị nhớ
612
Bộ điều khiển bộ nhớ SOC chốt khóa dữ liệu phản hồi và kiểm tra tín hiệu chỉ báo lỗi
614
Xác định xem có xảy ra lỗi hay không
616
không
có
Bộ điều khiển bộ nhớ SOC yêu cầu thông tin lỗi từ thiết bị nhớ
618
Bộ điều khiển bộ nhớ SOC lưu thông tin lỗi và kích hoạt ngắt vào SOC chính
620

FIG. 6

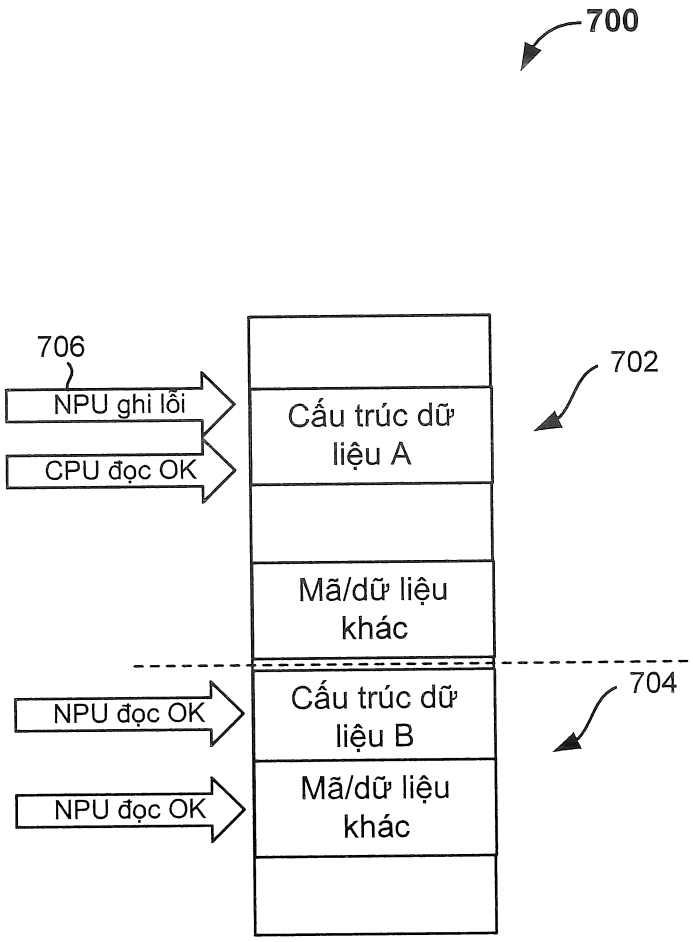
700
706
NPU ghi lỗi
CPU đọc OK
Cấu trúc dữ liệu A
Mã/dữ liệu khác
702
NPU đọc OK
NPU đọc OK
Cấu trúc dữ liệu B
Mã/dữ liệu khác
704

FIG. 7

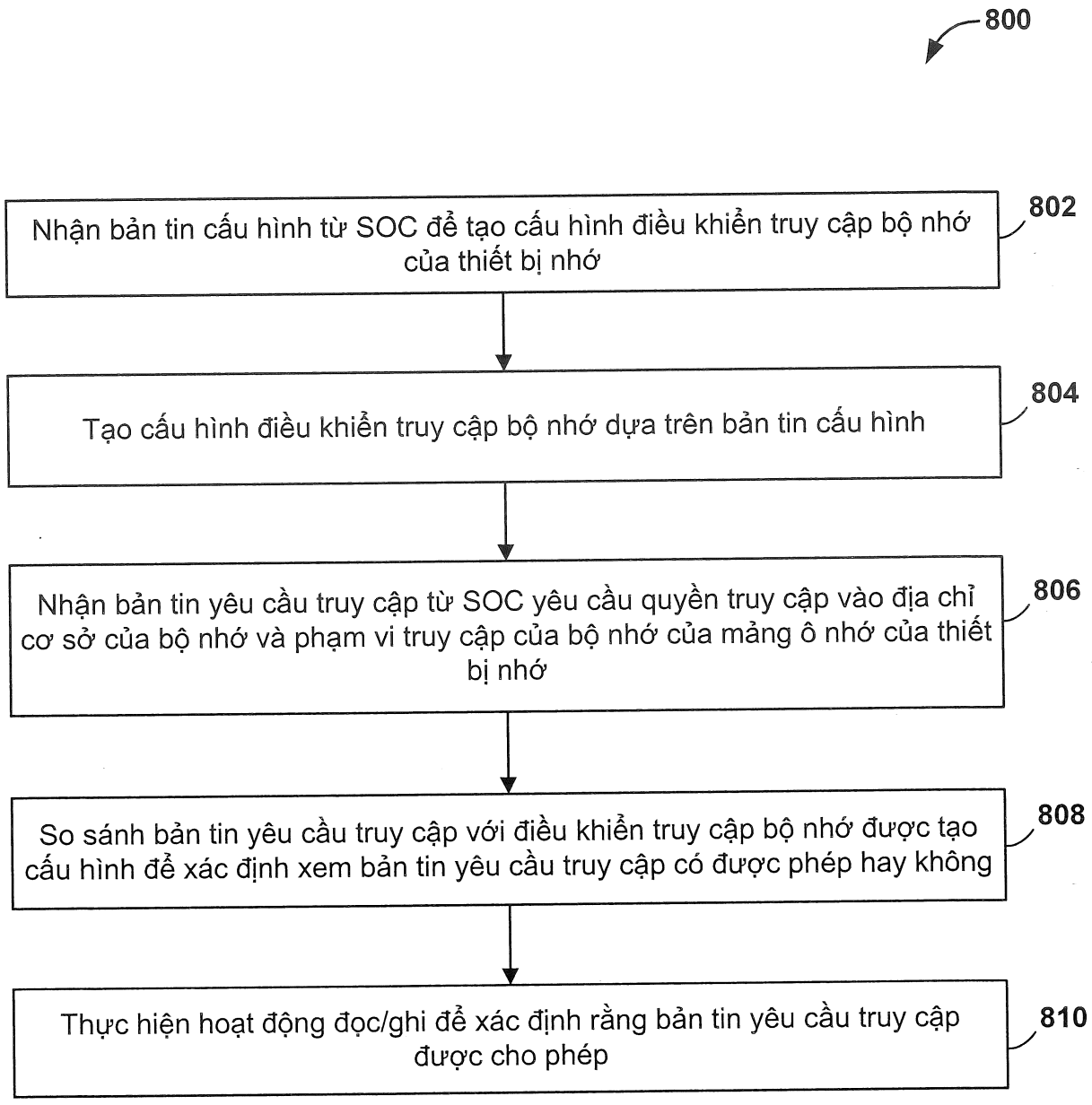
800
Nhận bản tin cấu hình từ SOC để tạo cấu hình điều khiển truy cập bộ nhớ của thiết bị nhớ
802
Tạo cấu hình điều khiển truy cập bộ nhớ dựa trên bản tin cấu hình
804
Nhận bản tin yêu cầu truy cập từ SOC yêu cầu quyền truy cập vào địa chỉ cơ sở của bộ nhớ và phạm vi truy cập của bộ nhớ của mảng ô nhớ của thiết bị nhớ
806
So sánh bản tin yêu cầu truy cập với điều khiển truy cập bộ nhớ được tạo cấu hình để xác định xem bản tin yêu cầu truy cập có được phép hay không
808
Thực hiện hoạt động đọc/ghi để xác định rằng bản tin yêu cầu truy cập được cho phép
810

FIG. 8

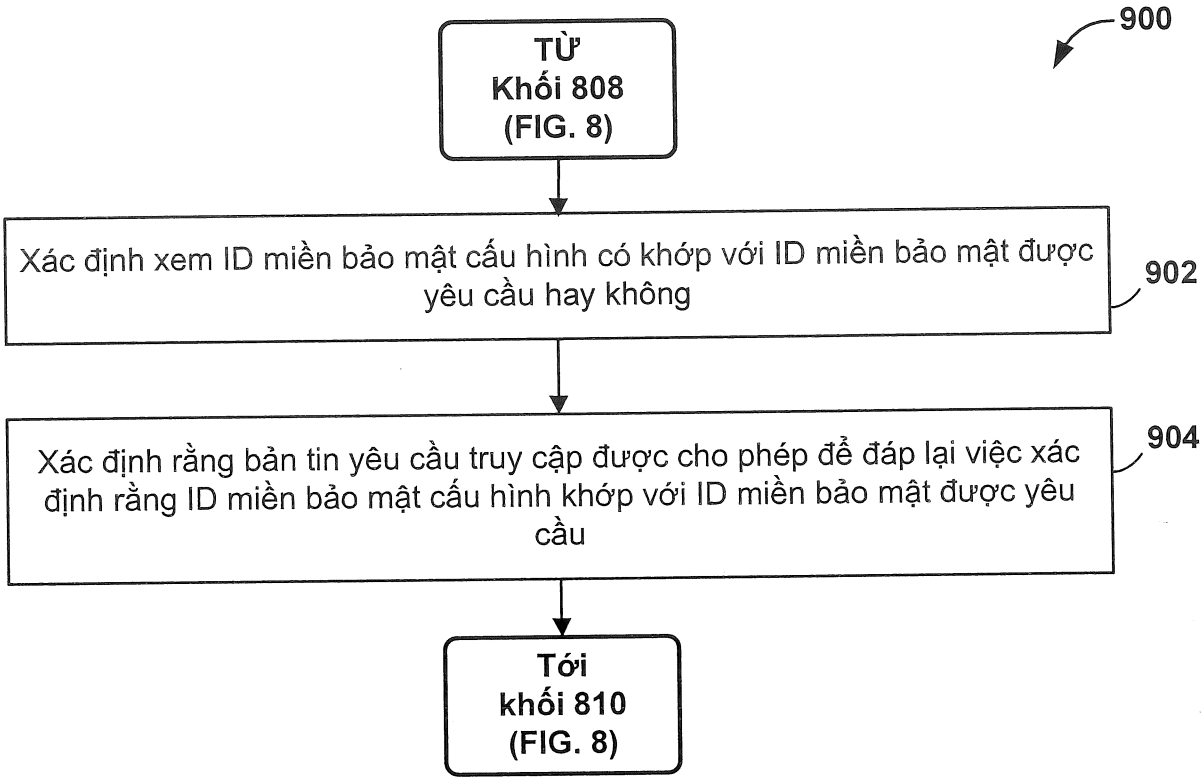
900
TỪ
Khối 808
(FIG. 8)
Xác định xem ID miền bảo mật cấu hình có khớp với ID miền bảo mật được yêu cầu hay không
902
Xác định rằng bản tin yêu cầu truy cập được cho phép để đáp lại việc xác định rằng ID miền bảo mật cấu hình khớp với ID miền bảo mật được yêu cầu
904
Tới
khối 810
(FIG. 8)

FIG. 9

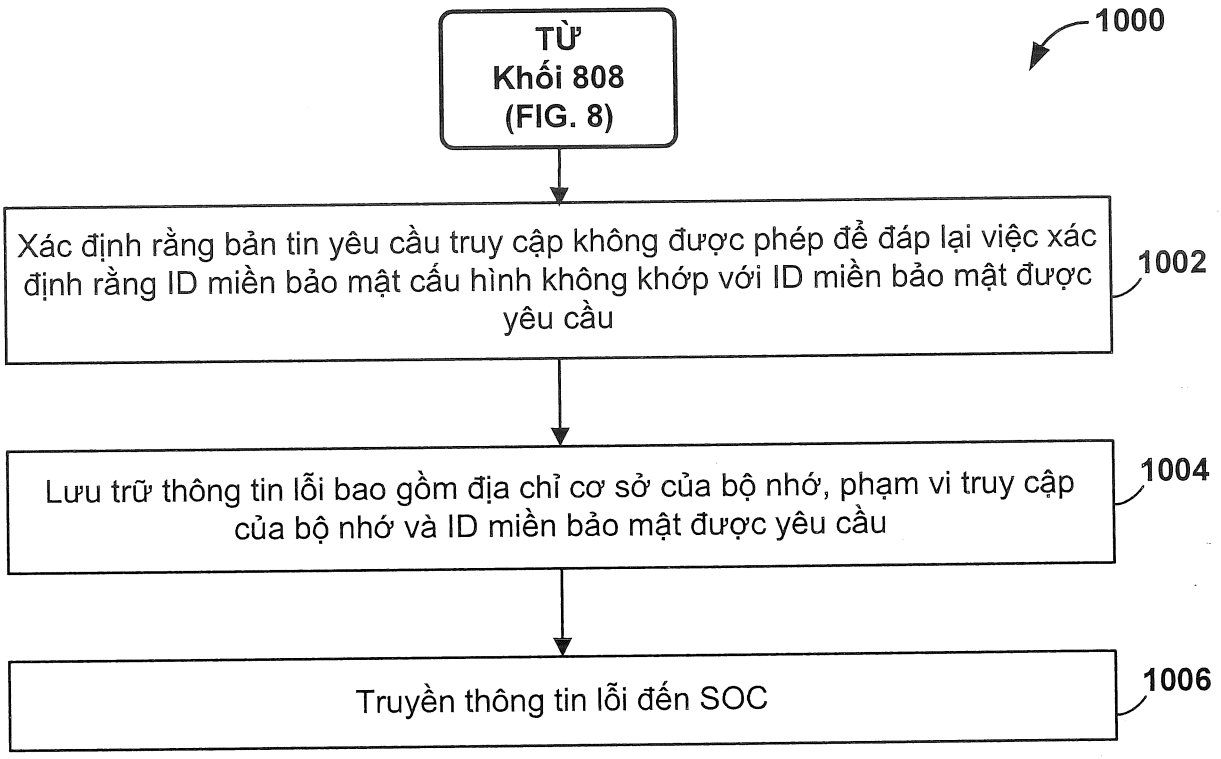
TỪ
Khối 808
(FIG. 8)
1000
Xác định rằng bản tin yêu cầu truy cập không được phép để đáp lại việc xác định rằng ID miền bảo mật cấu hình không khớp với ID miền bảo mật được yêu cầu
1002
Lưu trữ thông tin lỗi bao gồm địa chỉ cơ sở của bộ nhớ, phạm vi truy cập của bộ nhớ và ID miền bảo mật được yêu cầu
1004
Truyền thông tin lỗi đến SOC
1006

FIG. 10

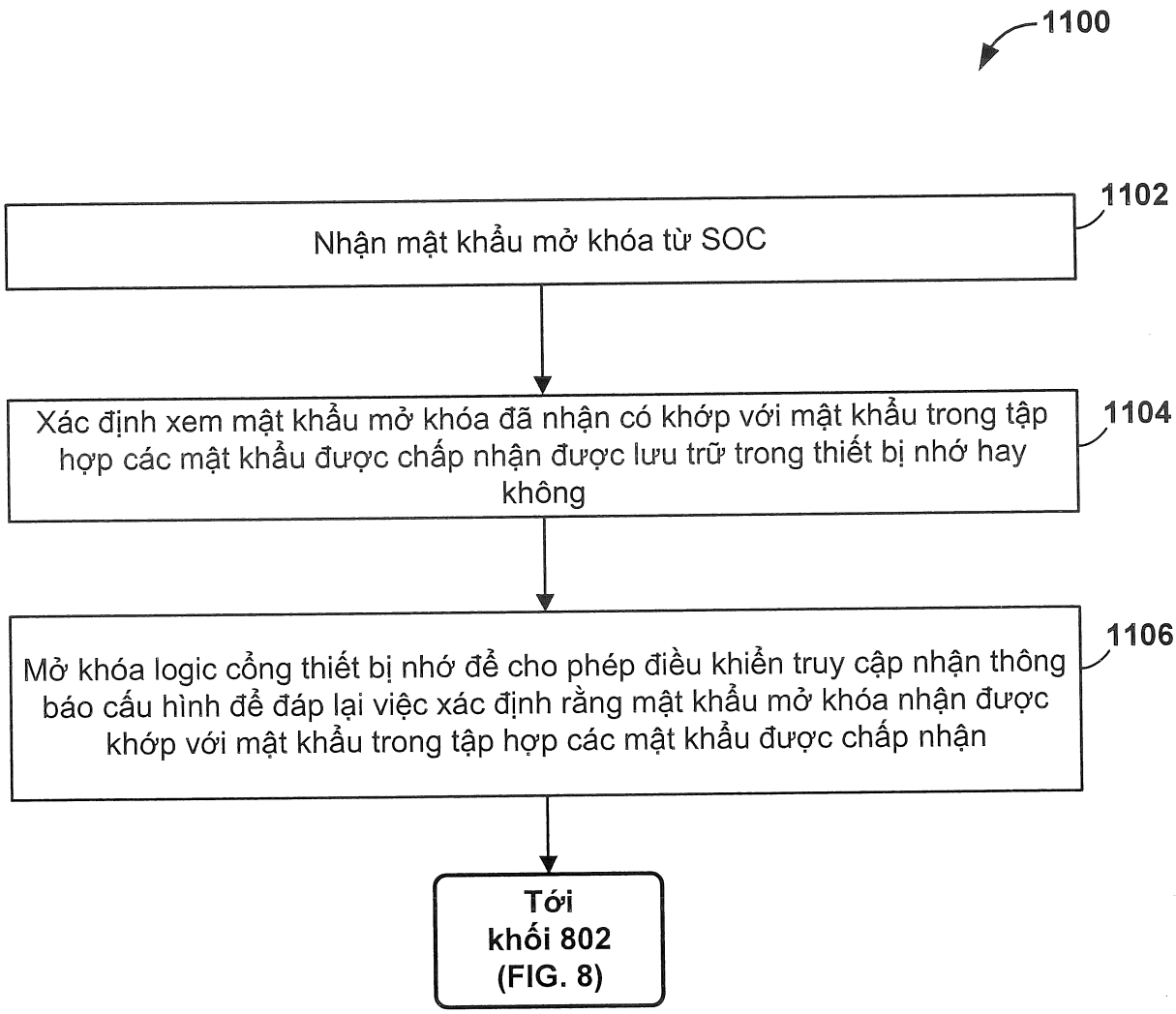
1100
1102
Nhận mật khẩu mở khóa từ SOC
1104
Xác định xem mật khẩu mở khóa đã nhận có khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận được lưu trữ trong thiết bị nhớ hay không
1106
Mở khóa logic cổng thiết bị nhớ để cho phép điều khiển truy cập nhận thông báo cấu hình để đáp lại việc xác định rằng mật khẩu mở khóa nhận được khớp với mật khẩu trong tập hợp các mật khẩu được chấp nhận
Tới khối 802 (FIG. 8)

FIG. 11

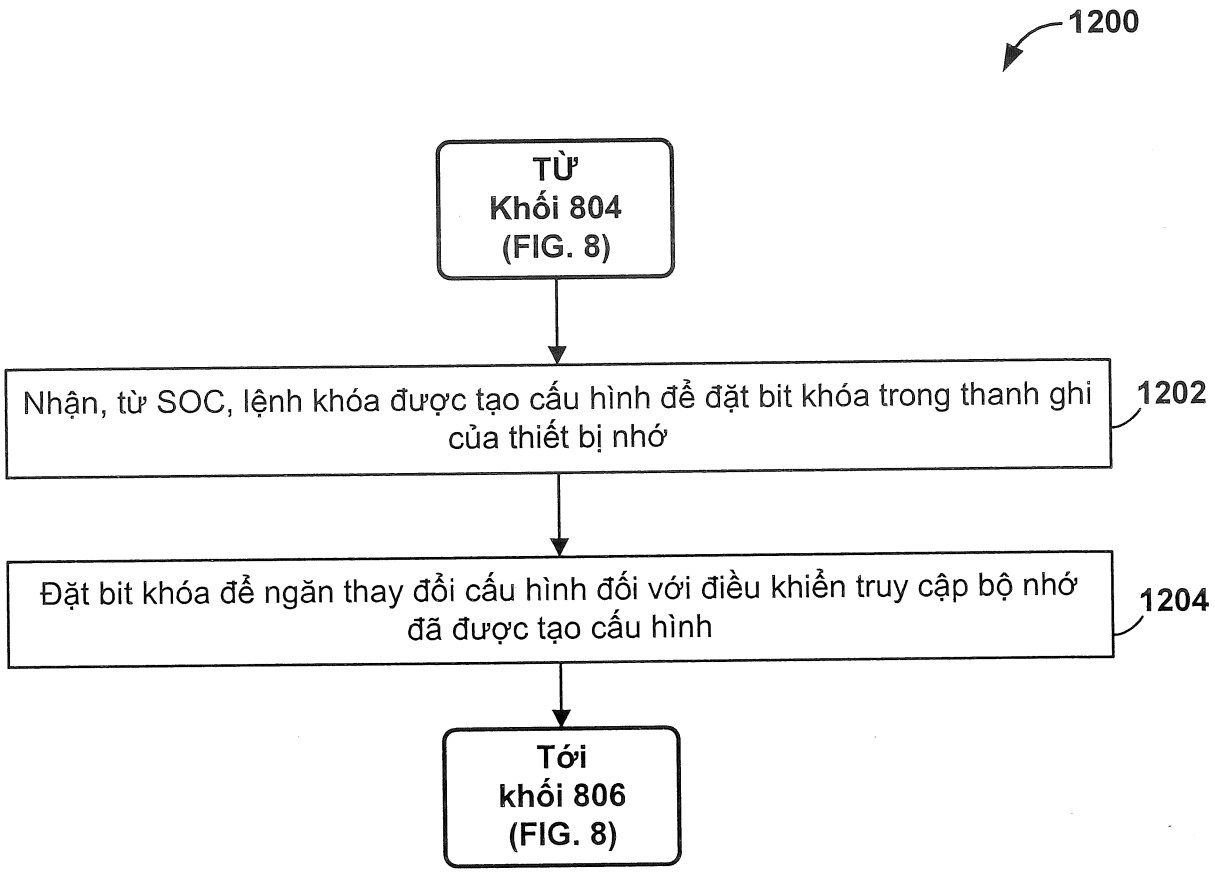
1200
TỪ
Khối 804
(FIG. 8)
Nhận, từ SOC, lệnh khóa được tạo cấu hình để đặt bit khóa trong thanh ghi của thiết bị nhớ
1202
Đặt bit khóa để ngăn thay đổi cấu hình đối với điều khiển truy cập bộ nhớ đã được tạo cấu hình
1204
Tới
khối 806
(FIG. 8)

FIG. 12

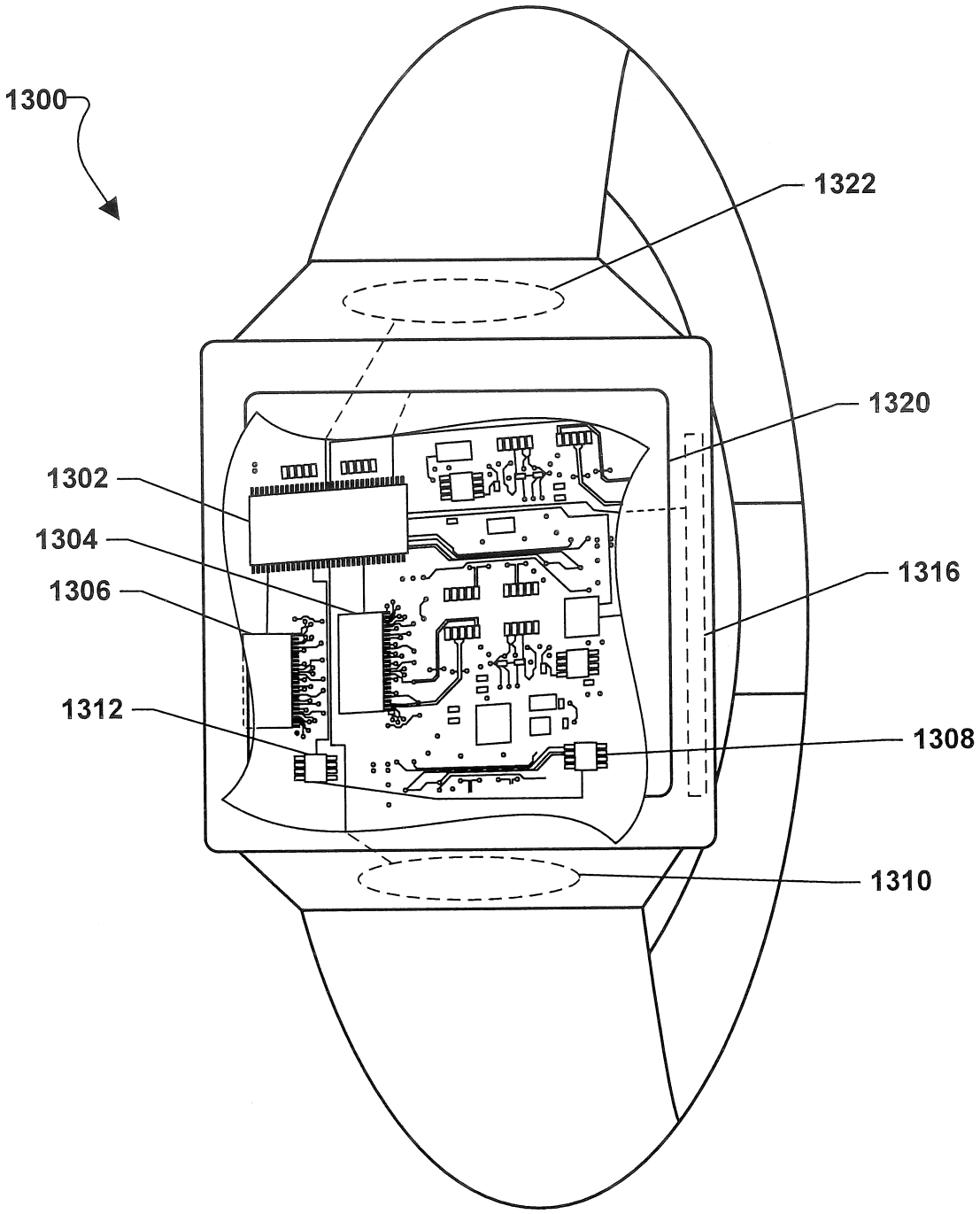

FIG. 13

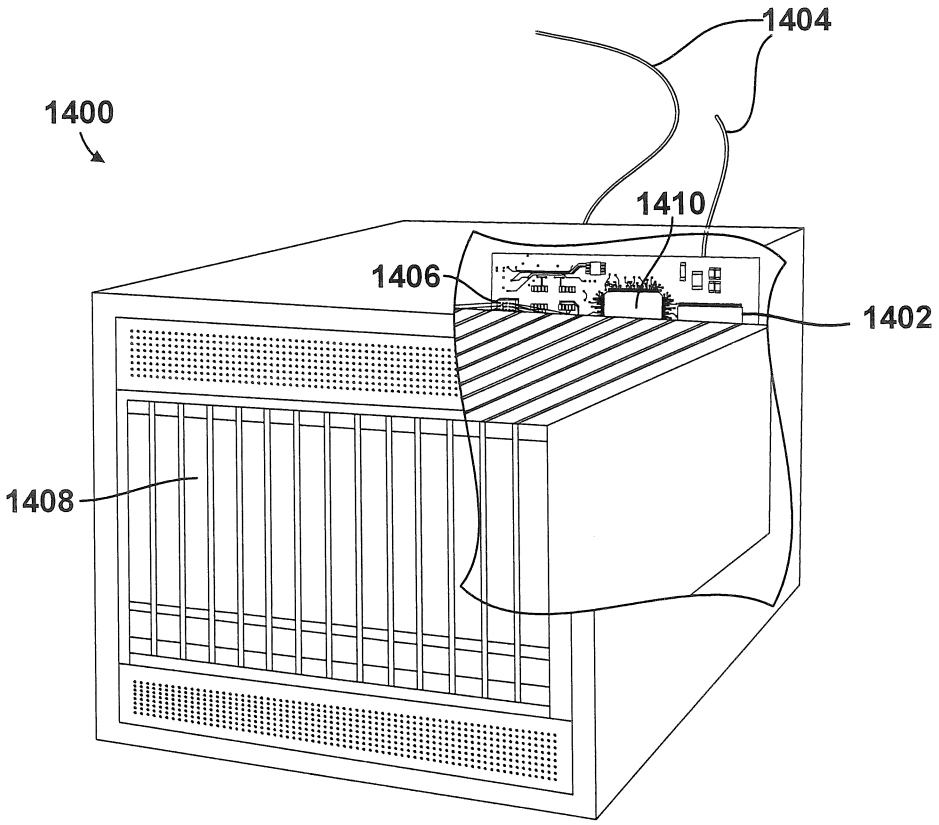

FIG. 14

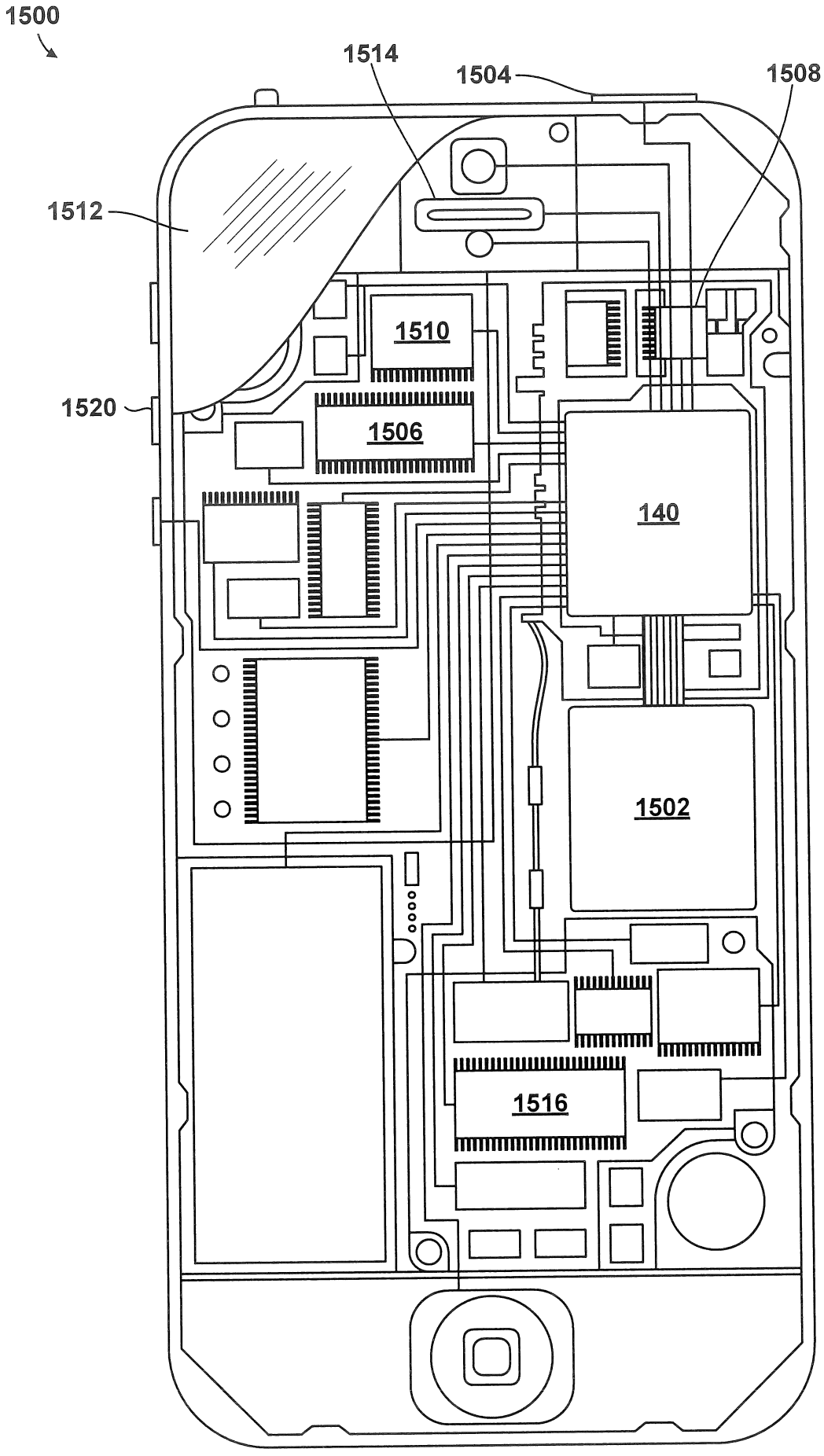

FIG. 15