MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA DI INVENZIONE NUMERO	**102022000002960**
Data Deposito	**17/02/2022**
Data Pubblicazione	**17/08/2023**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	12	109

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	12	14

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	13	28

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	13	42

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	12	02

Titolo

Sistema di elaborazione, relativo circuito integrato, dispositivo e procedimento

DESCRIZIONE dell'invenzione industriale dal titolo:
"Sistema di elaborazione, relativo circuito integrato, dispositivo e procedimento"
di: STMicroelectronics S.r.l., di nazionalità italiana, Via C. Olivetti, 2 – 20864 Agrate Brianza (Provincia di Monza e Brianza), Italia; STMicroelectronics SA, di nazionalità francese, 29 boulevard Romain Rolland, 92120 Montrouge, Francia.
Inventori designati: Roberta VITTIMANI, Federico GOLLER, Riccardo ANGRILLI, Charles AUBENAS
Depositata il: 17 febbraio 2022

* * *

TESTO DELLA DESCRIZIONE

Campo Tecnico

Le forme di attuazione della presente descrizione sono relative ai sistemi di elaborazione, come i microcontrollori.

Sfondo

La Figura 1 rappresenta un tipico sistema elettronico, come il sistema elettronico di un veicolo, comprendente una pluralità di sistemi di elaborazione 10, come sistemi embedded o circuiti integrati, per es., una FPGA (Field Programmable Gate Array), un DSP (Digital Signal Processor) o un microcontrollore (per es., dedicato al mercato automotive).

Per esempio, nella Figura 1 sono rappresentati tre sistemi di elaborazione 10_1, 10_2 e 10_3 connessi attraverso un sistema di comunicazione 20 adatto. Per esempio, il sistema di comunicazione può comprendere un bus di controllo del veicolo, come un bus CAN (Controller Area Network) e/o Ethernet, ed eventualmente un bus multimediale, come un bus

MOST (Media Oriented Systems Transport), connesso al bus di controllo del veicolo attraverso un gateway. Tipicamente, i sistemi di elaborazione 10 sono situati in differenti posizioni del veicolo e possono comprendere, per es., una Unità di Controllo del Motore ("Engine Control Unit"), una Unità di Controllo della Trasmissione (TCU, "Transmission Control Unit"), un Sistema Frenante Antiblocco (ABS, "Anti-lock Braking System"), un modulo di controllo della scocca (BCM, "Body Control Module") e/o un sistema audio multimediale e/o di navigazione. Di conseguenza, uno o più dei sistemi di elaborazione 10 possono anche implementare funzioni di controllo e di regolazione in tempo reale ("real-time"). Questi sistemi di elaborazione sono identificati di solito come Unità di Controllo Elettroniche (ECU, "Electronic Control Unit").

La Figura 2 rappresenta uno schema a blocchi di un esempio di un sistema di elaborazione 10 digitale, come un microcontrollore, che può essere usato come uno qualsiasi dei sistemi di elaborazione 10 della Figura 1.

Nell'esempio considerato, il sistema di elaborazione 10 comprende un microprocessore 102, di solito l'Unità di Elaborazione Centrale (CPU, "Central Processing Unit"), programmato mediante istruzioni software. Di solito, il software eseguito dal microprocessore 102 è memorizzato in una memoria di programma 104 non volatile, come una memoria Flash o una EEPROM. Così, la memoria 104 è configurata per memorizzare il firmware dell'unità di elaborazione 102, in cui il firmware comprende le istruzioni software che devono essere eseguite dal microprocessore 102. Generalmente, la memoria non volatile 104 può anche essere usata per memorizzare altri dati, come i dati di configurazione, per es., i dati di calibrazione.

Il microprocessore 102 ha di solito associata anche una memoria volatile 104b, come una memoria ad accesso casuale (RAM, "Random-Access-Memory"). Per esempio, la memoria 104b può essere usata per memorizzare dati temporanei.

Come rappresentato nella Figura 2, di solito la comunicazione con le memorie 104 e/o 104b è effettuata mediante uno o più controllori di memoria 100. Il controllore (i controllori) di memoria 100 può essere integrato (possono essere integrati) nel microprocessore 102 o connesso (connessi) al microprocessore 102 mediante un canale di comunicazione, come un bus di sistema del sistema di elaborazione 10. Similmente, le memorie 104 e/o 104b possono essere integrate con il microprocessore 102 in un singolo circuito integrato, o le memorie 104 e/o 104b possono essere sotto forma di un circuito integrato separato e connesso al microprocessore 102, per es., mediante le piste di una scheda a circuito stampato (PCB, "Printed Circuit Board").

Nell'esempio considerato, il microprocessore 102 può avere associate una o più risorse (hardware) 106, selezionate tra il gruppo di:

- una o più interfacce di comunicazione IF, per es. per scambiare dati tramite il sistema di comunicazione 20, come una interfaccia UART (Universal Asynchronous Receiver/ Transmitter), Bus SPI (Serial Peripheral Interface), I^2C (Inter-Integrated Circuit), bus CAN (Controller Area Network), e/o una interfaccia Ethernet e/o una interfaccia di debug; e/o

- uno o più convertitori analogico/digitali AD e/o convertitori digitale/analogici DA; e/o

- uno o più componenti digitali DC dedicati, come contatori e/o timer hardware, o un coprocessore crittografico; e/o

- uno o più componenti analogici AC, come comparatori, sensori, come un sensore di temperatura, ecc.; e/o

- uno o più componenti a segnali misti MSC, come un dispositivo di pilotaggio ("driver") PWM (Pulse-Width Modulation).

Generalmente, componenti digitali DC dedicati possono corrispondere anche a una FPGA integrata nel sistema di elaborazione 10. Per esempio, in questo caso, la memoria 104 può comprendere anche i dati di programma per una tale FPGA.

Di conseguenza, il sistema di elaborazione digitale 10 può supportare differenti funzionalità. Per esempio, il comportamento del microprocessore (dei microprocessori) 102 è determinato dal firmware memorizzato nella memoria 104, per es., le istruzioni software che devono essere eseguite da un microprocessore 102 di un microcontrollore 10. Così, installando un firmware differente, lo stesso (microcontrollore) hardware può essere usato per differenti applicazioni.

A questo riguardo, ci si aspetta che la futura generazione di tali sistemi di elaborazione 10, per es., microcontrollori atti a essere usati nelle applicazioni automotive, presenti un aumento della complessità, dovuto principalmente al numero crescente di funzionalità richieste (nuovi protocolli, nuove caratteristiche, ecc.) e ai vincoli stringenti delle condizioni di esecuzione (per es., un consumo di potenza più basso, una maggiore velocità e potenza di calcolo, ecc.).

Per esempio, recentemente sono stati proposti sistemi di elaborazione multi-core 10 più complessi. Per esempio, tali sistemi di elaborazione multi-core possono essere usati per eseguire (in parallelo) vari dei sistemi di elaborazione

10 rappresentati nella Figura 1, come vari sistemi di elaborazione di un veicolo.

La Figura 3 rappresenta un esempio di un sistema di elaborazione multi-core 10. Specificamente, nell'esempio considerato, il sistema di elaborazione 10 comprende una pluralità di *n* core di elaborazione 102_1...102_n, connessi a un sistema di comunicazione (on-chip) 114. Per esempio, nel contesto dei sistemi di controllo in tempo reale, i core di elaborazione 102_1...102_n possono essere dei core ARM Cortex®-R52. Generalmente, il sistema di comunicazione 114 può comprendere uno o più sistemi di bus, per es., basati su AXI (Advanced eXtensible Interface) e/o un NoC (Network-on-Chip).

Per esempio, come rappresentato nell'esempio del core di elaborazione 102_1, ciascun core di elaborazione 102 può comprendere un microprocessore 1020 e un'interfaccia di comunicazione 1022 configurata per gestire la comunicazione tra il microprocessore 1020 e il sistema di comunicazione 114. Tipicamente, l'interfaccia 1022 è un'interfaccia master configurata per inoltrare una data richiesta di (lettura o scrittura) dal microprocessore 1020 al sistema di comunicazione 114, e per inoltrare una risposta opzionale dal sistema di comunicazione 114 al microprocessore 1020. Tuttavia, ciascun microprocessore 1020 può avere anche associata un'interfaccia slave 1024. Per esempio, in questo modo, un primo microprocessore 1020 può inviare una richiesta a un secondo microprocessore 1020 (mediante l'interfaccia master 1022 del primo microprocessore, il sistema di comunicazione 114 e l'interfaccia slave 1024 del secondo microprocessore).

Generalmente, ciascun core di elaborazione 102_1...102_n può anche comprendere ulteriori risorse locali, come una o

più memorie locali 1026, identificata di solito come TCM (Tightly Coupled Memory).

Come menzionato in precedenza, tipicamente i core di elaborazione 102_1...102_n sono disposti per scambiare dati con una memoria non volatile 104 e/o una memoria volatile 104b. In un sistema di elaborazione multi-core 10, spesso queste memorie sono memorie di sistema, cioè, condivise per i core di elaborazione 102_1...102_n. Come menzionato in precedenza, ciascuno dei core di elaborazione 102_1...102_n può comprendere, tuttavia, una o più memorie locali 1026 aggiuntive.

Per esempio, come rappresentato nella Figura 3, il sistema di elaborazione 10 può comprendere uno o più controllori di memoria 100 configurati per connettere almeno una memoria non volatile 104 e almeno una memoria volatile 104b al sistema di comunicazione 114. Come menzionato in precedenza, una o più delle memorie 104 e/o 104b possono essere integrate nel circuito integrato del sistema di elaborazione 10 o connesse all'esterno del circuito integrato.

Come menzionato in precedenza, il sistema di elaborazione 10 può comprendere una o più risorse 106, come una o più interfacce di comunicazione o coprocessori (per es., un coprocessore crittografico). Le risorse 106 sono connesse di solito al sistema di comunicazione 114 mediante una rispettiva interfaccia di comunicazione slave 1064. Per esempio, in questo modo, un core di elaborazione 102 può inviare una richiesta a una risorsa 106 e la risorsa restituisce dati forniti. Per esempio, a questo scopo, il sistema di comunicazione 114 può comprendere in effetti un Bus ad Alte Prestazioni (AHB, "High-performance Bus") AMBA (Advanced Microcontroller Bus Architecture), e un Bus

Periferico Avanzato (APB, “Advanced Peripheral Bus”) usato per connettere le risorse/periferiche 106 al bus AHB AMBA.

Generalmente, una o più delle risorse 106 possono anche comprendere una rispettiva interfaccia master 1062, spesso identificato anche come controllore di Accesso Diretto in Memoria (DMA, “Direct-Memory-Access”) integrato. Per esempio, una tale interfaccia master 1062 può essere utile nel caso in cui la risorsa 106 debba iniziare una comunicazione al fine di scambiare dati mediante una richiesta (di lettura e/o di scrittura) con un altro circuito connesso al sistema di comunicazione 114, come una memoria 104/104b, una risorsa 106 o un core di elaborazione 102.

Spesso tali sistemi di elaborazione 10 comprendono anche uno o più controllori di Accesso Diretto in Memoria (DMA) non specializzati (“general-purpose”) 110. Generalmente, un controllore DMA non specializzato 110 può comprendere almeno un canale funzionale connesso a una risorsa 106. Spesso, la risorsa 106 associata a un dato canale può anche essere selezionata in funzione di dati di configurazione. Specificamente, un canale è un canale di lettura o di scrittura (che può anche essere programmabile) ed ha tipicamente dati di configurazione associati, che indicano:

- nel caso di un canale di lettura, l’intervallo di indirizzi di memoria da cui il controllore DMA 110 dovrebbe leggere dati; e

- nel caso di un canale di scrittura, l’intervallo di indirizzi di memoria in cui il controllore DMA 110 dovrebbe scrivere dati.

Per esempio, in questo modo, un’interfaccia di comunicazione IF può essere connessa al controllore DMA 110 mediante due canali:

- un canale di lettura configurato per leggere autonomamente dati da trasmettere da un primo intervallo di memoria nella memoria 104b e fornire i dati che sono stati letti all'interfaccia di comunicazione IF (che trasmette quindi i rispettivi dati); e

- un canale di scrittura configurato per ricevere dati che sono stati ricevuti dall'interfaccia di comunicazione IF e scrivere autonomamente questi dati in un secondo intervallo di memoria nella memoria 104b.

Di conseguenza, un controllore DMA 110 ha tipicamente associata un'interfaccia master 1102 per trasmettere le richieste di lettura o di scrittura al controllore di memoria 100. Generalmente, a questo scopo, l'interfaccia master 1102 può essere connessa mediante un canale DMA dedicato direttamente al controllore di memoria 110 o l'interfaccia master 1102 può inviare le richieste al sistema di comunicazione 114. Per esempio, in quest'ultimo caso, le richieste di lettura e di scrittura possono comprendere un qualsiasi indirizzo gestito dal sistema di comunicazione 114.

Similmente, invece di interfacciare direttamente una risorsa 106 mediante un canale dedicato, un controllore DMA non specializzato 110 può anche essere configurato per scambiare i dati con la risorsa 106 mediante il sistema di comunicazione 114. Per esempio, in questo caso, il controllore DMA 110 può essere configurato per inviare mediante l'interfaccia master 1102 dapprima una richiesta di lettura comprendente un primo indirizzo e poi una richiesta di scrittura comprendente un secondo indirizzo.

Di conseguenza, tipicamente un controllore DMA non specializzato 110 comprende anche un'interfaccia slave 1104

per ricevere dati di configurazione per configurare il controllore DMA 110.

Tipicamente, le interfacce slave, per es., le interfacce 1024, 1064 e/o 1104, sono configurate per interfacciare uno o più registri del rispettivo circuito. Per esempio, questi registri possono essere usati per memorizzare dati di configurazione per il rispettivo circuito e/o altri dati specifici per le risorse, come dati da trasmettere o ricevere nel caso di un'interfaccia di comunicazione o dati campionati nel caso di un ADC.

Specificamente, sebbene le interfacce slave siano rappresentate come blocchi integrati nel rispettivo circuito, in realtà un dato circuito può anche comprendere solo un'interfaccia a registri a uno o più registri del circuito, che è di solito il caso per i cosiddetti core IP. Di conseguenza, in questo caso, l'interfaccia slave può essere configurata per convertire le richieste scambiate mediante il sistema di comunicazione 114 in operazioni di lettura o di scrittura in questi uno o più registri. Di conseguenza, un'interfaccia slave può effettivamente fare parte del sistema di comunicazione 114, o può essere implementata in parte all'interno del sistema di comunicazione 114 e in parte nel rispettivo circuito.

Per esempio, di solito ciascuna richiesta di lettura o di scrittura comprende un indirizzo, in cui un indirizzo univoco del sistema di comunicazione 114 è associato a ciascun registro. Tipicamente, l'intervallo di indirizzi del sistema di comunicazione 114 è identificato come un intervallo di indirizzi fisici del sistema di elaborazione 10. Di conseguenza, un'interfaccia slave può essere configurata per gestire uno o più dei registri e per rilevare richieste comprendenti un indirizzo associato a un registro

gestito dall'interfaccia slave. Nel caso di una richiesta di lettura, l'interfaccia slave può così leggere il contenuto del registro associato all'indirizzo incluso nella richiesta, e può inviare il rispettivo contenuto, per es., mediante un rispettivo messaggio di risposta, al sistema di comunicazione 114. Per contro, nel caso di una richiesta di lettura, l'interfaccia slave può memorizzare i dati inclusi nella richiesta di scrittura nel registro associato all'indirizzo incluso nella richiesta. Per esempio, a questo scopo, una data interfaccia slave può monitorare gli scambi di comunicazioni mediante un bus 114. Per contro, nel caso di un'interconnessione di sistema, come un controllore di interconnessione di rete (NIC, "Network Interconnect Controller") o un NoC, almeno una parte dell'interfaccia slave può essere implementata effettivamente in un'interfaccia di comunicazione del NIC o del NoC tra un'interconnessione di sistema 114 e il rispettivo circuito.

Gli inventori hanno osservato che i registri dei vari circuiti del sistema di elaborazione 10 possono anche memorizzare dati, che possono essere rilevanti da un punto di vista della sicurezza. Per esempio, questo si applica a uno o più dei registri di un core di elaborazione 102, una risorsa 106 o un controllore DMA 110.

A questo riguardo, la protezione di accesso nei sistemi di elaborazione multi-core e/o nei sistemi di elaborazione che eseguono differenti compiti ("task") software o perfino macchine virtuali, è gestita di solito assegnando diritti di accesso a ciascun core di elaborazione 102, ciascuna macchina virtuale e/o ciascun compito software. Per esempio, in molti sistemi di elaborazione 10, questo problema è risolto usando una protezione di intervalli di indirizzi software e/o hardware.

Per esempio, l'architettura ARM AArch64 può usare un'architettura di sistema di memoria virtuale (VMSA, "Virtual Memory System Architecture"), in cui un'unità di gestione della memoria (MMU, "Memory Management Unit") di ciascun core di elaborazione 102 è usata per mappare indirizzi virtuali (VA, "Virtual Address") su indirizzi fisici (PA, "Physical Address") del sistema di comunicazione 114 mediante cosiddette tabelle di traduzione (TTB, "Translation TaBle"). A causa del fatto che gli intervalli di indirizzi fisici del sistema di comunicazione 114 sono associati a intervalli di memoria nelle memorie 104 e/o 104b, e nelle risorse 106, è possibile così limitare i diritti di accesso in lettura e in scrittura di una data applicazione APP o del sistema operativo OS a dati intervalli di memoria e/o date risorse 106.

Per contro, l'architettura ARM AArch32 usa tipicamente un'architettura di sistema di memoria protetta (PMSA, "Protected Memory System Architecture") invece di una VMSA. In questo caso, il sistema di elaborazione comprende un'unità di protezione della memoria (MPU, "Memory Protection Unit"). Specificamente, invece di definire la mappatura di indirizzi virtuali su indirizzi fisici, la MPU permette di specificare, per es., mediante una tabella, una o più regioni di memoria nello spazio degli indirizzi fisici e permette di specificare i rispettivi diritti di accesso e attributi di memoria. Per esempio, questa tabella dei diritti di accesso dell'OS e delle applicazioni APP può essere implementata nel livello di eccezione EL1.

Di conseguenza, usando una MMU o una MPU, il sistema di elaborazione 10 è configurato per inibire selettivamente l'inoltro di richieste da un'interfaccia master, per es., un'interfaccia master 1022 di un core di elaborazione 102,

al sistema di comunicazione 114. Per contro, la domanda di brevetto italiano numero 102021000011639 descrive una soluzione in cui una o più delle interfacce slave implementano una funzione di firewall, cioè, l'interfaccia slave stessa è configurata per inibire selettivamente l'inoltro di richieste dal sistema di comunicazione 114 al rispettivo circuito.

Di conseguenza, queste soluzioni permettono di definire i diritti di accesso, che possono essere usati per determinare se una richiesta di scrittura corrisponde a una richiesta di scrittura autorizzata generata da un core di elaborazione autorizzato, macchine virtuali e/o compiti software. Tuttavia, queste soluzioni non sono in grado di verificare se una richiesta di scrittura autorizzata è stata generata in realtà per errore o non intenzionalmente.

Sintesi

In considerazione di quanto precede, uno scopo delle varie forme di attuazione della presente descrizione è di fornire soluzioni migliorate per gestire gli accessi in scrittura a registri che contengono dati rilevanti per la sicurezza.

Secondo una o più forme di attuazione, uno o più degli scopi precedenti sono raggiunti per mezzo di un sistema di elaborazione avente le caratteristiche esposte specificamente nelle rivendicazioni che seguono. Le forme di attuazione concernono inoltre un relativo circuito integrato, dispositivo e procedimento.

Le rivendicazioni sono parte integrante dell'insegnamento tecnico della descrizione qui fornita.

Come menzionato in precedenza, varie forme di attuazione della presente descrizione sono relative a un sistema di elaborazione. Il sistema di elaborazione

comprende un sistema di comunicazione avente un dato intervallo di indirizzi fisici e un core di elaborazione comprendente un microprocessore configurato per eseguire istruzioni software ed avente associato un circuito di interfaccia master configurato per inoltrare richieste di scrittura dal microprocessore al sistema di comunicazione, in cui la richiesta di scrittura comprende un indirizzo fisico dell'intervallo di indirizzi fisici e dati da scrivere nell'indirizzo fisico.

Di conseguenza, un circuito può avere associato un circuito di interfaccia slave configurato per gestire un sotto-intervallo di indirizzi e inoltrare selettivamente richieste di scrittura indirizzate a un dato indirizzo dal sistema di comunicazione al circuito. Per esempio, il circuito può comprendere uno o più registri e uno o più circuiti periferici configurati per scambiare dati con l'uno o più registri. In questo caso, un rispettivo dato indirizzo può essere associato a ciascuno dell'uno o più registri e il circuito di interfaccia slave può essere configurato per inoltrare selettivamente le richieste di scrittura determinando il registro associato all'indirizzo estratto dalla richiesta di scrittura e memorizzando i dati estratti dalla richiesta di scrittura nel rispettivo registro. Per esempio, in varie forme di attuazione, il circuito di interfaccia slave è un dispositivo ponte ("bridge") periferico, in cui l'uno o più registri sono connessi al circuito di interfaccia slave mediante un bus periferico.

In varie forme di attuazione, il circuito di interfaccia slave ha associati dati di configurazione che indicano se il dato indirizzo è protetto o non protetto e comprende una memoria (volatile), per es., implementata con registri, per memorizzare dati di configurazione aggiuntivi che indicano

se il dato indirizzo è bloccato o sbloccato. Per esempio, i dati di configurazione possono indicare per ciascuno dell'uno o più registri se il rispettivo indirizzo è protetto o non protetto.

Specificamente, in varie forme di attuazione, il circuito di interfaccia slave è configurato per ricevere una richiesta di scrittura indirizzata al dato indirizzo dal sistema di comunicazione, estrarre dalla richiesta di scrittura ricevuta il rispettivo indirizzo e dati, e determinare se i dati di configurazione indicano che l'indirizzo estratto è protetto o non protetto, e se i dati di configurazione aggiuntivi indicano che l'indirizzo estratto è bloccato o sbloccato.

Specificamente, in risposta a una determinazione che l'indirizzo estratto non è protetto o che l'indirizzo estratto è sbloccato, il circuito di interfaccia slave può inoltrare la richiesta di scrittura al circuito. Per contro, in risposta a una determinazione che l'indirizzo estratto è protetto e che l'indirizzo estratto è bloccato, il circuito di interfaccia slave può generare un segnale di sblocco mediante un'operazione logica combinatoria.

Specificamente, in varie forme di attuazione, l'operazione logica combinatoria è configurata per confrontare l'indirizzo estratto con i dati estratti, asserendo con ciò il segnale di sblocco quando i dati estratti soddisfano una regola predeterminata rispetto all'indirizzo estratto. Di conseguenza, in varie forme di attuazione, la protezione può essere sbloccata quando i dati inclusi in una richiesta di scrittura soddisfano una data regola rispetto al rispettivo indirizzo incluso nella richiesta di scrittura, evitando con ciò il rischio che una data protezione sia sbloccata non intenzionalmente. Per

esempio, in varie forme di attuazione. il circuito di interfaccia slave è configurato per generare il segnale di sblocco confrontando uno o più bit dell'indirizzo estratto con uno o più bit dei dati estratti. Più specificamente, in varie forme di attuazione, il circuito di interfaccia slave è configurato per asserire il segnale di sblocco quando l'indirizzo estratto corrisponde ai dati estratti.

Di conseguenza, quando il segnale di sblocco è asserito, il circuito di interfaccia slave può aggiornare i dati di configurazione aggiuntivi al fine di indicare che l'indirizzo estratto è sbloccato. Per esempio, in varie forme di attuazione, i dati di configurazione aggiuntivi comprendono un valore di indirizzo temporaneo. In questo caso, il circuito di interfaccia slave può sbloccare un indirizzo estratto memorizzando l'indirizzo estratto come il valore di indirizzo temporaneo. Per esempio, in questo caso, il circuito di interfaccia slave può determinare se un indirizzo estratto è bloccato o sbloccato confrontando l'indirizzo estratto con il segnale di indirizzo temporaneo.

Per contro, quando il segnale di sblocco è deasserito, il circuito di interfaccia slave può aggiornare i dati di configurazione aggiuntivi al fine di indicare che l'indirizzo estratto è bloccato. Per esempio, al fine di bloccare l'indirizzo estratto, il circuito di interfaccia slave può aggiornare i dati di configurazione aggiuntivi al fine di indicare che tutti gli indirizzi gestiti dall'indirizzo dell'interfaccia slave sono bloccati.

In varie forme di attuazione, in risposta a una determinazione che l'indirizzo estratto non è protetto o che l'indirizzo estratto è sbloccato, che così implica che la richiesta di scrittura è inoltrata, il circuito di interfaccia slave può anche aggiornare i dati di

configurazione aggiuntivi al fine di indicare che l'indirizzo estratto è bloccato, bloccando di nuovo con ciò l'indirizzo una volta che la richiesta di scrittura è stata eseguita.

Breve descrizione delle figure

Forme di attuazione della presente descrizione saranno ora descritte con riferimento ai disegni annessi, che sono forniti puramente a titolo di esempio non limitativo, e nei quali:

- la Figura 1 rappresenta un esempio di un sistema elettronico comprendente una pluralità di sistemi di elaborazione;

- la Figura 2 rappresenta un esempio di un sistema di elaborazione, come un microcontrollore;

- la Figura 3 rappresenta un esempio di un sistema di elaborazione multi-core;

- la Figura 4 rappresenta una forma di attuazione di un sistema di elaborazione secondo la presente descrizione;

- la Figura 5 rappresenta una forma di attuazione di un'interfaccia slave, come un bridge periferico, per il sistema di elaborazione della Figura 4;

- la Figura 6 rappresenta una forma di attuazione di dati di configurazione usati per specificare i registri protetti per l'interfaccia slave della Figura 5;

- la Figura 7 rappresenta una forma di attuazione del funzionamento dell'interfaccia slave della Figura 5;

- le Figure 8 e 9 rappresentano una forma di attuazione di un'implementazione dell'interfaccia slave della Figura 5.

Descrizione Dettagliata

Nella descrizione che segue, sono illustrati numerosi dettagli specifici, allo scopo di fornire una comprensione approfondita delle forme di attuazione. Le forme di

attuazione possono essere attuate senza uno o più dei dettagli specifici o con altri procedimenti, componenti, materiali, ecc. In altri casi, operazioni, materiali o strutture ben note non sono rappresentate o descritte in dettaglio per evitare di rendere poco chiari certi aspetti delle forme di attuazione.

Un riferimento a "una forma di attuazione" in tutta questa descrizione intende indicare che una particolare configurazione, struttura, o caratteristica descritta con riferimento alla forma di attuazione è compresa in almeno una forma di attuazione. Così, le frasi come "in una forma di attuazione" o simili che compaiono in vari punti in tutta questa descrizione non fanno necessariamente riferimento tutte alla stessa forma di attuazione. Inoltre, particolari conformazioni, strutture o caratteristiche possono essere combinate in un modo adeguato qualsiasi in una o più forme di attuazione.

I riferimenti usati qui sono forniti semplicemente per convenienza e non definiscono l'ambito o il significato delle forme di attuazione.

Nelle Figure da 4 a 9 che seguono, le parti, gli elementi o i componenti che sono già stati descritti con riferimento alle Figure 1 e 3 sono indicati con gli stessi riferimenti usati precedentemente in tali Figure; la descrizione di tali elementi descritti precedentemente non sarà ripetuta in seguito al fine di non rendere troppo pesante la presente descrizione dettagliata.

Come menzionato in precedenza, varie forme di attuazione della presente descrizione sono relative a soluzioni per bloccare richieste di scrittura erronee o non volute inviate mediante un sistema di comunicazione di un sistema di elaborazione, come un microcontrollore.

La Figura 4 rappresenta una forma di attuazione di un sistema di elaborazione 10a secondo la presente descrizione. Specificamente, l'architettura generale del sistema di elaborazione 10a corrisponde all'architettura descritta con riferimento alla Figura 3, e la rispettiva descrizione si applica nella sua interezza.

Specificamente, anche in questo caso, il sistema di elaborazione 10a comprende:

- un sistema di comunicazione 114a, come un bus di sistema, un NIC o un NoC;
- uno o più core di elaborazione 102a, come core di elaborazione $102a_1$...$102a_n$, in cui ciascun core di elaborazione 102 comprende un microprocessore programmabile in software 1020, un'interfaccia master 1022 e opzionalmente un'interfaccia slave 1024a; e
- almeno una periferica/risorsa 106 avente un'interfaccia slave 1064a, e opzionalmente un'interfaccia master 1062.

In varie forme di attuazione, il sistema di elaborazione 10a comprende anche un controllore di memoria 100a comprendente un'interfaccia slave 1004a per ricevere richieste di lettura e/o di scrittura dal sistema di comunicazione 114a, in cui le richieste di lettura o di scrittura sono usate per leggere dati da o memorizzare dati in una memoria non volatile 104 e/o in una memoria volatile 104b.

In varie forme di attuazione, il sistema di elaborazione 10a comprende anche un controllore DMA 110a comprendente un'interfaccia master 1102 per inviare richieste di lettura e/o di scrittura al sistema di comunicazione 114a, e opzionalmente un'interfaccia slave 1104a per ricevere dati di configurazione per il controllore DMA 110a.

Generalmente, un'interfaccia slave, come un'interfaccia slave 1004a, 1024a, 1104a o 1064a, ha associato un rispettivo indirizzo fisico o intervallo di indirizzi del sistema di comunicazione 114a. Per esempio, questo è rappresentato nella Figura 5 in cui un'interfaccia slave 1064a associata a una risorsa 106a ha associato un rispettivo indirizzo fisico o intervallo di indirizzi PA_106. Generalmente, ciascuna interfaccia slave ha associato un indirizzo o intervallo di indirizzi differente e univoco all'interno dell'intervallo di indirizzi fisici del sistema di comunicazione 114a, cioè, le varie interfacce slave hanno associati indirizzi o intervalli di indirizzi non in sovrapposizione.

Specificamente, come rappresentato nella Figura 5 nell'esempio di un'interfaccia slave 1064a, una data interfaccia slave può essere associata a una o più risorse 106a o altri circuiti del sistema di elaborazione 10a, per es., risorse $106a_1$, $106a_2$ e $106a_3$, in cui ciascuna risorsa/ciascun circuito comprende uno o più registri 1070. Generalmente, ciascun circuito/ciascuna risorsa comprende anche un circuito 1072 configurato per scambiare dati con l'uno o più rispettivi registri 1070. Per esempio, in linea con la descrizione della Figura 2, nel caso di una risorsa/periferica 106a, il circuito 1072 può essere un'interfaccia di comunicazione IF, un convertitore da analogico a digitale AD, un convertitore da digitale ad analogico DA, un componente digitale DC dedicato, un componente analogico AC o un componente a segnali misti MSC. Di conseguenza, ciascun registro 1070 può essere usato per memorizzare dati da fornire al circuito 1072, come dati di configurazione o dati che devono essere trasmessi e/o elaborati dal circuito 1072, e/o dati ricevuti dal circuito

1072, come dati ricevuti, campionati e/o elaborati dal circuito 1072.

Di conseguenza, in varie forme di attuazione, ciascuno dei registri 1070 gestiti da una data interfaccia slave può avere associato un rispettivo indirizzo univoco e può essere configurato per ricevere, mediante il sistema di comunicazione 114a, una richiesta di lettura e/o di scrittura. In risposta alla ricezione di una richiesta di lettura o di scrittura, l'interfaccia slave può determinare l'indirizzo incluso nella richiesta e determinare se l'indirizzo è associato a un registro 1070 gestito dall'interfaccia slave. Di conseguenza, in risposta a una determinazione che la richiesta è una richiesta di lettura comprendente un indirizzo associato a un dato registro 1070 gestito dall'interfaccia slave, l'interfaccia slave può leggere il contenuto del dato registro 1070 e inviare il contenuto del dato registro 1070 all'interfaccia di comunicazione 114a, per es., mediante un pacchetto di risposta. Per contro, in risposta a una determinazione che la richiesta è una richiesta di scrittura comprendente un indirizzo associato a un dato registro 1070 gestito dall'interfaccia slave, l'interfaccia slave può memorizzare i dati inclusi nella richiesta di scrittura nel dato registro 1070.

Generalmente, un qualsiasi sistema di comunicazione 1074 adeguato può essere usato per scambiare dati tra l'interfaccia slave e i registri 1070 gestiti da una data interfaccia slave. Per esempio, l'interfaccia slave può comunicare in modo indipendente (mediante connessioni dedicate) con uno o più dei registri 1070 gestiti e/o l'interfaccia slave può essere connessa a uno o più dei registri 1070 mediante un bus. Per esempio, in varie forme

di attuazione, l'interfaccia slave 1064a può essere una cosiddetta interfaccia di bus periferico, in cui l'interfaccia slave 1064a è connessa ai registri 1070 gestiti mediante uno o più sistemi di bus 1074, detti di solito bus periferici. Di conseguenza, l'interfaccia slave 1064a può essere un bridge periferico configurato per interfacciare il sistema di comunicazione 114a, come un NIC o un NoC, con una pluralità di risorse/periferiche 106a instradando le richieste di lettura o di scrittura (cioè, le transazioni) a uno o più dei registri 1070. Generalmente, un'interfaccia slave può anche elaborare i dati ricevuti, per es., al fine di effettuare un'operazione di conversione di protocollo, verificare uno o più bit di codice di correzione di errore (ECC, "Error Correction Code") inclusi nelle richieste, e/o aggiungere uno o più bit di ECC a un pacchetto di risposta.

Di conseguenza, un'interfaccia master, come un'interfaccia master 1022, 1062 o 1102, può essere configurata per inviare richieste di lettura RREQ o richieste di scrittura WREQ al sistema di comunicazione 114a e ricevere infine una rispettiva risposta alla richiesta dal sistema di comunicazione 114a. Di conseguenza, in questo modo, un microprocessore 1020 può programmare un dato registro 1070 di una risorsa 106a inviando una richiesta di scrittura WREQ al sistema di comunicazione 114a, in cui la richiesta di scrittura comprende l'indirizzo fisico associato al rispettivo registro 1070 e gestito dall'interfaccia slave 1064a associata alla risorsa 106a.

Come menzionato in precedenza, in un sistema critico per la sicurezza, modifiche indesiderate di uno o più dei registri del sistema di elaborazione 10a possono avere come risultato una situazione pericolosa. Per esempio, questo può

essere il caso per un sottoinsieme dei registri 1070 delle risorse/periferiche 106a.

Specificamente, in varie forme di attuazione, almeno una delle interfacce slave del sistema di elaborazione 10a, come l'interfaccia slave 1064a, ha associati dati di configurazione 1068, che specificano i registri 1070 gestiti dalle interfacce slave da proteggere.

Generalmente, i dati di configurazione per ciascun registro 1070 gestito da un'interfaccia slave possono essere fissati, per es., cablati in hardware ("hardwired"), o possono essere programmabili, cioè, l'interfaccia slave 1070 può essere configurata per:

- abilitare sempre la protezione per un dato registro 1070, cioè, senza considerare i dati di configurazione 1068;
- abilitare la protezione per un dato registro 1070 in funzione dei dati di configurazione 1068; o
- disabilitare sempre la protezione per un dato registro 1070, cioè, senza considerare i dati di configurazione 1068.

Per esempio, la Figura 6 rappresenta una forma di attuazione dei dati di configurazione 1068 per una pluralità di registri 1070 gestiti dall'interfaccia slave.

Specificamente, nella forma di attuazione considerata, i dati di configurazione 1068 comprendono per ciascun registro 1070 gestito dall'interfaccia slave uno o più rispettivi bit P, che specificano se la protezione dovrebbe essere disabilitata o abilitata per il rispettivo registro, per es., come i bit P1, P2 e P3 per i registri 1070_1, 1070_2 e 1070_3.

In varie forme di attuazione, i dati di configurazione 1068 possono anche comprendere uno o più bit EN che specificano se l'interfaccia slave dovrebbe considerare i

bit di configurazione P. Per esempio, in questo modo, l'interfaccia slave può essere configurata per:

- quando il (i) bit di abilitazione EN hanno un primo valore, per es., EN = "0", disabilitare la protezione per i registri 1070 gestiti; e

- quando il (i) bit di abilitazione EN hanno un secondo valore, per es., EN = "1", abilitare selettivamente la protezione per ciascun registro 1070 in funzione del rispettivo (dei rispettivi) bit P.

Come menzionato in precedenza, in varie forme di attuazione, uno o più dei bit dei dati di configurazione 1068 possono essere fissati (per es., cablati in hardware) o programmabili. Per esempio, in varie forme di attuazione, almeno una parte dei bit P può essere cablata in hardware, perché i registri 1070 rilevanti per la sicurezza possono essere determinati durante la fase di progetto. A questo riguardo, la programmabilità dei bit dei dati di configurazione 1068 può essere implementata:

- usando dati di configurazione, che sono letti mediante un circuito hardware dedicato da una memoria non volatile (per es., la memoria 104) durante l'avvio del sistema di elaborazione, come dati di configurazione programmati da un produttore del circuito integrato del sistema di elaborazione 10a; e/o

- usando come registro 1068 un registro che è programmabile inviando richieste di scrittura, per es., mediante un microprocessore 1020, al sistema di comunicazione 114a.

La Figura 7 rappresenta a questo riguardo una forma di attuazione del funzionamento dell'interfaccia slave, per es., l'interfaccia slave 1064a, come un bridge periferico.

Specificamente, dopo una fase di inizio 2000, che può corrispondere, per es., all'avvio del sistema di elaborazione, l'interfaccia slave procede a una fase di attesa 2002 al fine di attendere una nuova richiesta di scrittura WREQ a un indirizzo ADR gestito dall'interfaccia slave.

Per esempio, in varie forme di attuazione, la fase di attesa 2002 può essere implementata con una fase di verifica, dove l'interfaccia slave verifica se è stata ricevuta una richiesta di scrittura WREQ e, una volta che ha ricevuto una richiesta di scrittura, se la richiesta di scrittura WREQ comprende un indirizzo ADR gestito dall'interfaccia slave. Di conseguenza, nel caso in cui l'interfaccia slave non abbia ricevuto una richiesta di scrittura WREQ a un indirizzo gestito dall'interfaccia slave (uscita "N" della fase di verifica 2002), l'interfaccia slave ritorna alla fase 2002.

Per contro, nel caso in cui l'interfaccia slave abbia ricevuto una richiesta di scrittura WREQ a un indirizzo gestito dall'interfaccia slave (uscita "Y" della fase di verifica 2002), l'interfaccia slave procede a una fase 2004. Specificamente, nella forma di attuazione considerata, l'interfaccia slave è configurata per determinare nella fase 2004 l'indirizzo ADR della richiesta di scrittura WREQ e determinare, in base ai dati di configurazione 1068, se la protezione per il registro 1070 associato all'indirizzo di ricezione ADR è abilitata o disabilitata, per es., usando i dati EN e/o P menzionati precedentemente.

Inoltre, l'interfaccia slave legge nella fase 2004 dati di configurazione CFG aggiuntivi. Specificamente, i dati di configurazione CFG aggiuntivi corrispondono a dati temporanei che sono usati per indicare se un dato registro protetto 1070 è in uno stato di bloccato o in uno stato di

sbloccato. Per esempio, in varie forme di attuazione, i dati di configurazione aggiuntivi possono indicare un indirizzo TADR che indica l'indirizzo di un registro e opzionalmente un indicatore ("flag") di stato LSTAT che indica se l'indirizzo TADR è bloccato o sbloccato. Per esempio, quando si usa solo l'indirizzo TADR, l'indirizzo TADR può indicare che:

- tutti i registri protetti gestiti dall'interfaccia slave sono nello stato di bloccato, cioè, quando l'indirizzo TADR è impostato a un valore non gestito dall'interfaccia slave, per es., zero, o

- un singolo registro protetto gestito dall'interfaccia slave è nello stato di sbloccato, cioè, quando l'indirizzo TADR è impostato all'indirizzo del rispettivo registro.

Di conseguenza, in varie forme di attuazione, l'interfaccia slave può verificare in una fase 2006 se il registro associato all'indirizzo ADR incluso nella richiesta di scrittura WREQ è protetto e se il rispettivo registro è bloccato o sbloccato. Per esempio, a questo scopo l'interfaccia slave può usare i dati EN e/o P dei dati 1068 al fine di determinare se il registro è protetto, e confrontare l'indirizzo temporaneo TADR con l'indirizzo ADR incluso nella richiesta, e opzionalmente verificare il valore dell'indicatore LSTAT.

Nel caso in cui l'interfaccia slave determini che il registro 1070 associato all'indirizzo ADR incluso nella richiesta di scrittura WREQ non è protetto o che la protezione sia sbloccata (uscita "N" della fase di verifica 2006), per es., perché l'indirizzo temporaneo TADR corrisponde all'indirizzo ADR incluso nella richiesta di scrittura WREQ e opzionalmente l'indicatore LSTAT indica che la protezione è sbloccata, l'interfaccia slave procede a una

fase 2012. Specificamente, l'interfaccia slave è configurata per eseguire la richiesta di scrittura nella fase 2012, cioè, memorizzare i dati DATA inclusi nella richiesta di scrittura (o i dati generati in funzione di questi dati DATA) nel registro 1070 associato all'indirizzo ADR incluso nella richiesta di scrittura.

Inoltre, in varie forme di attuazione, l'interfaccia slave blocca di nuovo, in una fase 2014, il rispettivo registro protetto o preferibilmente tutti i registri protetti, per es., resettando l'indirizzo TADR e/o l'indicatore di stato LSTAT. Generalmente, la fase 2014 può essere eseguita prima, dopo o in parallelo alla fase 2012.

Di conseguenza, una volta che la richiesta di scrittura è stata eseguita, l'interfaccia slave può ritornare alla fase 2002 per ricevere una successiva richiesta di scrittura WREQ.

Per contro, nel caso in cui l'interfaccia slave determini che il registro 1070 associato all'indirizzo ADR incluso nella richiesta di scrittura WREQ è protetto e la protezione è bloccata (uscita "Y" della fase di verifica 2006), per es., perché i dati di configurazione EN e/o P indicano che il registro è protetto e l'indirizzo temporaneo TADR non corrisponde all'indirizzo ADR incluso nella richiesta di scrittura WREQ o l'indicatore LSTAT opzionale indica che la protezione non è sbloccata, l'interfaccia slave procede a una fase di verifica 2008.

Specificamente, nella forma di attuazione considerata, l'interfaccia slave verifica nella fase 2008 se la protezione del registro associato all'indirizzo ADR incluso nella richiesta di scrittura WREQ dovrebbe essere sbloccata. Specificamente, a questo scopo, l'interfaccia slave può verificare una o più condizioni nella fase 2008.

Per esempio, in modo simile a una protezione con password, l'interfaccia slave potrebbe essere configurata per verificare, nella fase 2008, se una data password o chiave di riferimento è fornita con la richiesta WREQ, che permette di sbloccare la protezione. Tuttavia, gli inventori hanno osservato che questa soluzione può non essere adeguata al fine di proteggere i registri 1070 da accessi in scrittura non intenzionali. In effetti, una volta che è stata fornita la chiave di riferimento, tutti i registri 1070 gestiti dall'interfaccia slave sarebbero sbloccati. Di conseguenza, al fine di proteggere individualmente ciascun registro 1070 da operazioni di scrittura non volute, ciascun registro 1070 dovrebbe essere protetto mediante una rispettiva chiave di riferimento, per es., l'indirizzo TADR e opzionalmente l'indicatore LSTAT potrebbero essere impostati quando è fornita una data chiave di riferimento per lo specifico registro 1070. Tuttavia, questo implica che sarebbe richiesto un numero significativo di chiavi di riferimento, il che aumenta in modo apprezzabile la complessità del circuito di interfaccia slave.

A questo riguardo, gli inventori hanno osservato che una soluzione con bassa complessità può essere implementata usando l'indirizzo associato a un dato registro stesso come chiave di riferimento per sbloccare l'accesso in scrittura al dato registro.

Di conseguenza, in varie forme di attuazione, l'interfaccia slave è configurata per determinare l'indirizzo ADR e i dati DATA inclusi nella richiesta di scrittura WREQ, e l'interfaccia slave è configurata per determinare nella fase 2008 se i dati DATA concordano con/corrispondono all'indirizzo del registro protetto 1070, il che può anche essere verificato implicitamente

confrontando i dati DATA di una richiesta di scrittura WREQ con il rispettivo indirizzo ADR della stessa richiesta di scrittura WREQ. Di conseguenza, in varie forme di attuazione, un dato registro protetto 1070 è sbloccato quando sono soddisfatte le seguenti condizioni combinate:

- è ricevuta una richiesta di scrittura WREQ, in cui la richiesta di scrittura WREQ comprende un indirizzo ADR e dati DATA;

- l'indirizzo ADR corrisponde all'indirizzo associato al registro 1070; e

- i dati DATA corrispondono all'indirizzo associato al registro 1070.

In varie forme di attuazione, invece di verificare che l'indirizzo del registro 1070 o l'indirizzo ADR della richiesta di scrittura WREQ corrisponde ai dati DATA, l'interfaccia slave può anche confrontare, nella fase 2008, soltanto un sottoinsieme dei bit, per es., nel caso in cui il campo di indirizzo ADR abbia 16 bit e il campo di dati abbia 32 bit, e/o elaborare l'indirizzo ADR e/o i dati DATA e confrontare l'indirizzo ADR elaborato con i dati DATA elaborati. Per esempio, l'interfaccia slave può verificare, nella fase 2008, se:

- i dati DATA hanno valori di bit invertiti dell'indirizzo ADR; o

- i dati DATA corrispondono a una sequenza di bit che ha un ordine invertito dal bit più significativo a quello meno significativo rispetto all'indirizzo ADR.

Di conseguenza, in varie forme di attuazione, l'interfaccia slave verifica nella fase 2008, preferibilmente mediante un circuito logico combinatorio, se è soddisfatta una regola predeterminata, in cui questa regola confronta il contenuto dell'indirizzo ADR con i dati DATA,

per es., il circuito logico combinatorio può ricevere l'indirizzo ADR e i dati DATA e può generare un segnale UNLOCK che indica se il registro 1070 associato all'indirizzo ADR dovrebbe essere sbloccato. A questo riguardo, è vantaggiosa un'operazione di confronto di bit diretto tra uno o più bit dell'indirizzo ADR e uno o più bit dei dati DATA, perché il rispettivo circuito logico combinatorio può essere implementato con meno porte logiche combinatorie, che non introducono anche un ritardo di propagazione apprezzabile.

Di conseguenza, nel caso in cui l'interfaccia slave determini che il registro protetto dovrebbe essere sbloccato (uscita "Y" della fase di verifica 2008), l'interfaccia slave procede a una fase 2016, dove l'interfaccia slave scrive i dati di configurazione CFG aggiuntivi al fine di indicare che il registro associato all'indirizzo ADR incluso nella richiesta di scrittura è sbloccato, per es., memorizzando il valore ADR nel valore TADR e opzionalmente asserendo l'indicatore LSTAT. Per esempio, a questo scopo, l'interfaccia slave può comprendere un registro interno configurato per fornire il valore TADR memorizzando l'indirizzo ADR in risposta al segnale UNLOCK menzionato precedentemente.

Per contro, nel caso in cui l'interfaccia slave determini che il registro protetto non dovrebbe essere sbloccato (uscita "N" della fase di verifica 2008), l'interfaccia slave può procedere alla fase 2002 per attendere una nuova richiesta di scrittura o alla fase 2014 per bloccare di nuovo tutti i registri protetti. Per esempio, a questo scopo, l'interfaccia slave può resettare, nella fase 2014, il registro usato per memorizzare l'indirizzo TADR e/o l'indicatore LSTAT.

Di conseguenza, in varie forme di attuazione, il meccanismo di protezione funziona mediante due accessi in scrittura. Quando l'indirizzo ADR di una (prima) richiesta di scrittura WREQ corrisponde all'indirizzo associato a un registro protetto e bloccato (fase 2006), la richiesta di scrittura WREQ non è eseguita, ma i dati DATA della richiesta di scrittura WREQ sono usati per decidere se sbloccare il rispettivo registro protetto.

Specificamente, quando i dati DATA e l'indirizzo ADR soddisfano una data regola predeterminata (fase 2008), per es., quando i bit dei dati DATA corrispondono ai bit dell'indirizzo ADR, l'interfaccia slave rimuove il blocco per il dato registro nella fase 2016. In varie forme di attuazione, in questo caso, l'interfaccia slave può anche rispondere, per es., nella fase 2016, con un messaggio che indica che la richiesta è stata eseguita.

Per contro, quando i dati DATA e l'indirizzo ADR non soddisfano la data regola predeterminata (fase 2008), l'interfaccia slave non sblocca il registro protetto. In varie forme di attuazione, in questo caso, l'interfaccia slave può anche rispondere, per es., in una fase 2010 opzionale, con un messaggio che indica che la richiesta non è stata eseguita.

Di conseguenza, quando l'indirizzo ADR di una (seconda) richiesta di scrittura WREQ corrisponde all'indirizzo associato a un registro non protetto o sbloccato (fase 2006), la richiesta di scrittura WREQ è eseguita, per es., i dati DATA sono memorizzati nel rispettivo registro 1070. Come menzionato in precedenza, in varie forme di attuazione può essere sbloccato soltanto un singolo registro protetto 1070. Di conseguenza, le operazioni di scrittura in altri registri bloccati non saranno elaborate.

La Figura 8 rappresenta una possibile forma di attuazione di un circuito di interfaccia slave secondo la presente descrizione, come un'interfaccia slave 1064a.

Specificamente, nella forma di attuazione considerata, il sistema di comunicazione 114a è configurato per fornire all'interfaccia slave 1064a i seguenti segnali per ciascuna delle richieste di scrittura WREQ:

- un segnale MSEL usato per segnalare una richiesta, per es., asserendo il segnale MSEL;

- un segnale MW_R che indica se la richiesta è una richiesta di scrittura WREQ (per es., asserendo il segnale W_R) o una richiesta di lettura RREQ;

- segnali MDATA comprendenti i dati da scrivere;

- segnali MADR comprendenti l'indirizzo ADR in cui dovrebbero essere scritti i dati DATA.

Generalmente, questi segnali possono essere generati direttamente da un'interfaccia master connessa a un sistema di bus 114a, o i segnali possono essere generati da un'interfaccia di rete perimetrale ("edge network interface") di un NIC o un NoC.

Inoltre, in varie forme di attuazione, il sistema di comunicazione 114a può essere configurato per ricevere dall'interfaccia slave 1064a un segnale MRESP opzionale che indica una risposta di stato alla richiesta. Generalmente, la comunicazione può anche essere basata su ulteriori segnali che non sono rappresentati nella Figura 8, come un segnale RDATA per i dati di una richiesta di lettura RREQ e/o bit di ECC aggiuntivi.

Nella forma di attuazione considerata, l'interfaccia slave 1064a comprende una tradizionale interfaccia slave 1064 e un circuito di protezione 1076 configurato per gestire

il meccanismo di protezione in base ai dati di configurazione 1068.

Specificamente, l'interfaccia slave 1064 è configurata per ricevere i seguenti segnali:

- un segnale SSEL usato per segnalare una richiesta, per es., asserendo il segnale SEL;

- un segnale SW_R che indica se la richiesta è una richiesta di scrittura WREQ (per es., quando il segnale W_R è asserito) o una richiesta di lettura RREQ;

- segnali SDATA comprendenti i dati da scrivere;

- segnali SADR comprendenti l'indirizzo ADR in cui dovrebbero essere scritti i dati DATA.

Inoltre, in varie forme di attuazione, l'interfaccia slave 1064 può essere configurata per generare un segnale SRESP opzionale che indica una risposta di stato per la richiesta.

Di conseguenza, in un'interfaccia slave 1064 di tecnica nota tradizionale, i segnali MADR, MDATA, MW_R, MRESP e MSEL sarebbero connessi (per es., direttamente) ai segnali SADR, SDATA, SW_R, SRESP e SSEL, rispettivamente. Per contro, nella forma di attuazione considerata, il segnale SSEL e opzionalmente il segnale MRESP sono generati dal circuito di protezione 1076 in funzione dei segnali MSEL, MW_R, MADR, MREQ e opzionalmente SRESP.

La Figura 9 rappresenta una possibile forma di attuazione per il circuito di protezione 1076.

Specificamente, nella forma di attuazione considerata, l'indirizzo MADR e i dati MDATA sono forniti a un circuito di gestione del blocco 1080. Specificamente, nella forma di attuazione considerata, il circuito 1080 è configurato per generare un segnale di blocco LOCK e/o un segnale di sblocco UNLOCK confrontando i segnali MDATA e MADR quando è ricevuta

una nuova richiesta di scrittura WREQ, per es., quando il segnale MW_R è asserito e opzionalmente quando il segnale MSEL è asserito.

Specificamente, quando è ricevuta una richiesta di scrittura, il circuito di gestione del blocco 1080 può essere configurato per memorizzare l'indirizzo MADR in un registro 1090, in cui il registro 1090 fornisce il valore di indirizzo temporaneo TADR menzionato in precedenza che indica l'indirizzo di un indirizzo sbloccato. Per esempio, nella forma di attuazione considerata, il registro 1090 è configurato per memorizzare l'indirizzo MADR in risposta al segnale di sblocco UNLOCK, in cui il circuito 1080 asserisce il segnale di UNLOCK in risposta a una determinazione che i segnali MSEL e MW_R sono asseriti, e i segnali MDATA corrispondono ai segnali MADR. Di conseguenza, il circuito di gestione del blocco 1080 può essere implementato con un (semplice) circuito logico combinatorio.

Come menzionato in precedenza, in varie forme di attuazione il registro 1090 potrebbe essere resettato in risposta al segnale di blocco LOCK (fase 2014 della Figura 7). Per contro, nella forma di attuazione considerata, il registro 1090 non è resettato, ma è usato un registro 1078 aggiuntivo per memorizzare esplicitamente lo stato di blocco LSTAT. Generalmente, come rappresentato mediante un circuito logico combinatorio 1077, può essere usata una soluzione adeguata qualsiasi per memorizzare un indicatore LSTAT che indica se la protezione è bloccata o sbloccata. Per esempio, in varie forme di attuazione, il circuito di protezione 1076 comprende un flip flop set-reset 1078, in cui l'ingresso di set è connesso al segnale UNLOCK e l'ingresso di reset è connesso al segnale LOCK, per cui il segnale LSTAT è asserito

per segnalare uno stato di sbloccato. Tuttavia, il segnale LSTAT potrebbe anche indicare lo stato di bloccato.

Di conseguenza, nella forma di attuazione considerata, il circuito di protezione 1076 comprende anche un circuito (o un filtro di transazione) di verifica della protezione 1088 configurato per generare un segnale UNLOCKED che indica se l'accesso a un dato indirizzo è permesso/sbloccato.

Specificamente, nella forma di attuazione considerata, il circuito 1088 è configurato per ricevere il valore TADR che indica un indirizzo sbloccato (dal registro 1090), l'indirizzo MADR che indica l'indirizzo della richiesta di scrittura WREQ, i dati di configurazione 1068 che indicano quali indirizzi sono protetti o non protetti e opzionalmente lo stato di blocco LSTAT (per es., nel caso in cui lo stato di blocco non possa essere ricavato dal valore TADR).

Specificamente, in varie forme di attuazione, il circuito 1088 è configurato per determinare, in base al segnale MADR e ai dati di configurazione 1068, se l'indirizzo MADR corrente è protetto o non protetto. Inoltre, in varie forme di attuazione, il circuito 1088 è configurato per determinare, in base al segnale MADR e al valore TADR (e opzionalmente LSTAT), se la protezione dell'indirizzo MADR corrente è bloccata o sbloccata. Di conseguenza, in varie forme di attuazione, il circuito 1088 può asserire il segnale UNLOCKED in risposta a una determinazione che l'indirizzo MADR non è protetto o che la protezione dell'indirizzo MADR è sbloccata. Di conseguenza, anche il circuito di filtro di transazione 1088 può essere implementato con un (semplice) circuito logico combinatorio.

Di conseguenza, nella forma di attuazione considerata, il segnale SSEL può essere asserito quando il segnale MSEL è asserito e il segnale UNLOCKED è asserito, segnalando con

ciò la richiesta di scrittura WREQ all'interfaccia slave 1064 soltanto nel caso in cui il segnale UNLOCKED sia asserito. Per esempio, ipotizzando che un segnale sia asserito mediante il livello logico "1", il segnale SSEL può essere generato mediante una porta logica AND 1086 che riceve in ingresso i segnali MSEL e UNLOCKED.

Come menzionato in precedenza, in varie forme di attuazione, il circuito slave 1064 può anche generare un segnale di risposta SRESP. In questo caso, il circuito di protezione 1076 può comprendere un circuito generatore di risposta di blocco 1082. Specificamente, come menzionato in precedenza, la risposta MRESP fornita al sistema di comunicazione 114a dovrebbe corrispondere:

- nel caso in cui la richiesta di scrittura sia fornita all'interfaccia slave 1064, alla risposta SRESP fornita dall'interfaccia slave 1064;

- nel caso in cui la richiesta di scrittura abbia come risultato uno sblocco della protezione, a una risposta che indica un'esecuzione corretta del comando (di sblocco); e

- altrimenti, a una risposta che indica un errore nell'esecuzione del comando (di sblocco).

Specificamente, nella forma di attuazione considerata, il circuito generatore di risposta di blocco 1082 comprende:

- un circuito logico combinatorio 1094 configurato per generare un segnale di risposta URESP a un comando di sblocco, per es., il segnale URESP corrisponde alla versione invertita del segnale UNLOCK; e

- un multiplexer 1092 che fornisce in uscita il segnale MRESP selezionando il segnale URESP o SRESP in funzione del segnale SSEL che indica se la richiesta di scrittura è inoltrata all'interfaccia slave 1064.

Generalmente, a causa del fatto che la risposta dovrebbe essere fornita di solito soltanto con il prossimo ciclo di clock, il circuito di protezione 1076 può comprendere uno o più registri o flip-flop, come un flip-flop 1084 usato per memorizzare il valore del segnale SSEL (che indica se la richiesta di scrittura è inoltrata all'interfaccia slave 1064), e il multiplexer può usare il segnale SSEL memorizzato fornito dal flip-flop 1084.

Di conseguenza, anche l'implementazione del circuito rappresentata nella Figura 9 permette di specificare mediante i dati di configurazione 1068 un insieme di indirizzi da proteggere, per es., usando una mappa di bit comprendente un bit P per ciascun indirizzo gestito dall'interfaccia slave 1064.

Quando l'indirizzo MADR di una transazione di scrittura (come segnalato mediante i segnali MW_R e MSEL) corrisponde a un indirizzo protetto e la protezione è bloccata (come segnalato, per es., mediante il segnale LSTAT), la transazione è bloccata dal circuito 1088 mediante il segnale UNLOCKED.

In parallelo, il circuito 1080 usa i dati MDATA al fine di decidere se sbloccare la protezione. Specificamente, quando i dati MDATA sono uguali all'indirizzo MADR, il blocco è rimosso per l'indirizzo MADR, per es., aggiornando il valore TADR e opzionalmente il segnale LSTAT. Opzionalmente, il circuito 1082 può anche generare una risposta che indica che il comando di sblocco è stato eseguito.

Altrimenti, il blocco è confermato, per es., rispondendo mediante il circuito 1082 con uno stato di errore.

Per contro, quando l'indirizzo MADR di una transazione di scrittura (come segnalato mediante i segnali MW_R e MSEL)

corrisponde a un indirizzo non protetto, o a un indirizzo protetto e la protezione è sbloccata (come segnalato, per es., mediante il valore TADR e il segnale LSTAT opzionale), il circuito 1088 permette un instradamento della richiesta di scrittura all'interfaccia slave 1064, per es., mediante il segnale UNLOCKED. In questo caso, il circuito 1082 fornisce la risposta SRESP generata dall'interfaccia slave 1064 al sistema di comunicazione 114a.

Come rappresentato schematicamente nella Figura 7 mediante una fase 2003, l'interfaccia slave può anche essere configurata per verificare uno o più diritti di accesso.

Per esempio, la domanda di brevetto italiano numero 102021000011639 menzionata precedentemente descrive una soluzione in cui una o più delle interfacce slave implementano una funzione di firewall, cioè, l'interfaccia slave può essere configurata per inibire selettivamente, nella fase 2003, l'inoltro di una richiesta di lettura RREQ o di una richiesta di scrittura WREQ al rispettivo registro 1070. Specificamente, secondo questo documento, che è incorporato qui tramite citazione a questo scopo, il sistema di elaborazione 10a può comprendere un sistema di comunicazione 114a avente un dato intervallo di indirizzi fisici, e uno o più core di elaborazione 102a, in cui ciascun core di elaborazione 102a comprende almeno un microprocessore 1020 configurato per eseguire istruzioni software. Specificamente, ciascun microprocessore 1020 ha associato un circuito di interfaccia master 1022 configurato per inoltrare richieste di lettura o di scrittura dal microprocessore 1020 al sistema di comunicazione 114a, in cui le richieste di lettura o di scrittura comprendono un indirizzo fisico dell'intervallo di indirizzi fisici del sistema di comunicazione 114a.

Di conseguenza, in linea con la descrizione precedente, un circuito slave, come una risorsa/periferica 106a o un controllore di memoria 100a, può avere associato un circuito di interfaccia slave, per es., l'interfaccia slave 1064a, configurato per inoltrare selettivamente richieste di lettura o di scrittura indirizzate a un dato sotto-intervallo di indirizzi dal sistema di comunicazione 114a al primo circuito.

Specificamente, secondo il documento 102021000011639, il circuito di interfaccia master del microprocessore 1020 ha associato un registro per memorizzare un rispettivo ID di macchina virtuale (VMID, "Virtual Machine ID") e/o un ID di spazio degli indirizzi (ASID, "Address Space ID"). Specificamente, in varie forme di attuazione, il circuito di interfaccia master di un microprocessore 1020 è configurato per leggere il VMID e/o l'ASID dal registro e inserire il VMID e/o l'ASID nelle richieste di lettura o di scrittura inoltrate dal microprocessore 1020 al sistema di comunicazione 114a, cioè, il VMID e/o l'ASID sono trasmessi con le richieste. Similmente, anche altri circuiti di interfaccia master, per es., di altri core di elaborazione 102a e/o un controllore DMA 110, possono inserire un rispettivo VMID e/o ASID nelle richieste.

Di conseguenza, in varie forme di attuazione, il circuito di interfaccia slave può determinare se la richiesta è autorizzata. Specificamente, a questo scopo, in varie forme di attuazione, il circuito di interfaccia slave ha associato un registro per memorizzare dati di configurazione di sicurezza SECS (si veda anche la Figura 5), per es., una lista 1066 di VMID e/o di ASID autorizzati, in cui ciascun elemento della lista 1066 è associato a un dato indirizzo o

sotto-intervallo di indirizzi gestito dall'interfaccia slave.

Specificamente, in questo caso, il circuito di interfaccia slave può essere configurato per ricevere una richiesta di lettura o di scrittura indirizzata al dato indirizzo o sotto-intervallo di indirizzi dal sistema di comunicazione 114, estrarre dalla richiesta ricevuta il VMID e/o l'ASID, determinare il VMID e/o l'ASID autorizzati associati al dato indirizzo o sotto-intervallo di indirizzi in funzione dei dati di configurazione di sicurezza SECS e determinare se il VMID e/o l'ASID virtuali estratti dalla richiesta ricevuta corrispondono al VMID e/o all'ASID autorizzati, rispettivamente.

Per esempio, in risposta a una determinazione che il VMID e/o l'ASID estratti dalla richiesta ricevuta corrispondono al VMID e/o all'ASID autorizzati, il circuito di interfaccia slave può inoltrare la richiesta di lettura o di scrittura al circuito slave. Per contro, in risposta a una determinazione che il VMID e/o l'ASID estratti dalla richiesta ricevuta non corrispondono al VMID e/o all'ASID autorizzati, il circuito di interfaccia slave può inibire l'inoltro della richiesta di lettura o di scrittura al primo circuito, per es., può rifiutare la richiesta di lettura o di scrittura.

Per esempio, usando il VMID, è possibile specificare se il microprocessore 1020 e un dato circuito slave appartengono alla stessa macchina virtuale.

Per esempio, al fine di combinare il meccanismo di protezione da operazioni di scrittura non volute con il meccanismo di autenticazione, il circuito 1088 potrebbe asserire il segnale UNLOCKED soltanto quando anche il VMID e/o l'ASID estratti dalla richiesta ricevuta corrispondono

ai rispettivi VMID e/o ASID autorizzati indicati dai dati di configurazione di sicurezza SECS. In alternativa, può essere usato un circuito separato per l'autenticazione, in cui il circuito aggiuntivo genera un segnale che indica un accesso autorizzato, e in cui questo segnale è fornito alla porta logica 1086.

Naturalmente, fermi restando i principi di fondo dell'invenzione, i dettagli di costruzione e le forme di attuazione possono variare, anche in modo apprezzabile, rispetto a quanto è stato descritto e illustrato qui, puramente a titolo di esempio, senza uscire con ciò dall'ambito della presente invenzione, come definito dalle rivendicazioni che seguono.

RIVENDICAZIONI

1. Sistema di elaborazione (10a) comprendente:

- un sistema di comunicazione (114a) avente un dato intervallo di indirizzi fisici (PA);

- un core di elaborazione (102a) comprendente un microprocessore (1020) configurato per eseguire istruzioni software ed avente associato un circuito di interfaccia master (1022) configurato per inoltrare richieste di scrittura (WREQ) da detto microprocessore (1020) a detto sistema di comunicazione (114a), dette richieste di scrittura (WREQ) comprendendo un indirizzo fisico (ADR; MADR) di detto intervallo di indirizzi fisici e dati (DATA; MDATA) da scrivere in detto indirizzo fisico (ADR; MADR); e

- un circuito (100a, 102a, 106a, 110a) avente associato un circuito di interfaccia slave (1004a, 1024a, 1064a, 1104a) configurato per gestire un sotto-intervallo di indirizzi (PA_106) e inoltrare selettivamente richieste di scrittura (WREQ) indirizzate a un dato indirizzo da detto sistema di comunicazione (114a) a detto circuito (100a, 102a, 106a, 110a);

in cui detto circuito di interfaccia slave (1064a) ha associati dati di configurazione (1068; EN, P) che indicano se detto dato indirizzo è protetto o non protetto e comprende una memoria (1078, 1090) per memorizzare dati di configurazione (CFG; TADR, LSTAT) aggiuntivi che indicano se detto dato indirizzo è bloccato o sbloccato, e in cui detto circuito di interfaccia slave (1064a) è configurato per:

- ricevere (2002) una richiesta di scrittura (WREQ) indirizzata a detto dato indirizzo da detto sistema di comunicazione (114a),

- estrarre da detta richiesta di scrittura (WREQ) ricevuta il rispettivo indirizzo (ADR; MADR) e dati (DATA; MDATA),

- determinare (2004, 2006) se detti dati di configurazione (1068; EN, P) indicano che l'indirizzo (ADR; MADR) estratto è protetto o non protetto, e se detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi indicano che l'indirizzo (ADR; MADR) estratto è bloccato o sbloccato;

- in risposta a una determinazione che l'indirizzo estratto (ADR; ADR) non è protetto o che l'indirizzo (ADR; MADR) estratto è sbloccato, inoltrare (2012) detta richiesta di scrittura (WREQ) a detto circuito (100a, 102a, 106a, 110a);

- in risposta a una determinazione che l'indirizzo (ADR; MADR) estratto è protetto e che l'indirizzo (ADR; MADR) estratto è bloccato, generare un segnale di sblocco (UNLOCK; LOCK) mediante un'operazione logica combinatoria (1080) configurata per confrontare detto indirizzo (ADR; MADR) estratto con detti dati (DATA; MDATA) estratti, asserendo con ciò detto segnale di sblocco (UNLOCK; LOCK) quando detti dati (DATA; MDATA) estratti soddisfano una regola predeterminata rispetto a detto indirizzo (ADR; MADR) estratto, e:

- quando detto segnale di sblocco (UNLOCK; LOCK) è asserito, aggiornare (2016) detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi al fine di indicare che l'indirizzo (ADR; MADR) estratto è sbloccato, e

- quando detto segnale di sblocco (UNLOCK; LOCK) è deasserito, aggiornare (2014) detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi al fine di

indicare che l'indirizzo (ADR; MADR) estratto è bloccato.

2. Sistema di elaborazione (10a) secondo la Rivendicazione 1, in cui detto circuito di interfaccia slave (1064a) è configurato per:

- in risposta a una determinazione che l'indirizzo estratto (ADR; ADR) non è protetto o che l'indirizzo (ADR; MADR) estratto è sbloccato, aggiornare (2014) detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi al fine di indicare che l'indirizzo (ADR; MADR) estratto è bloccato.

3. Sistema di elaborazione (10a) secondo la Rivendicazione 1 o la Rivendicazione 2, in cui detto aggiornare (2014) detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi al fine di indicare che l'indirizzo (ADR; MADR) estratto è bloccato comprende:

- aggiornare (2014) detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi al fine di indicare che tutti gli indirizzi gestiti da detto circuito di interfaccia slave (1064a) sono bloccati.

4. Sistema di elaborazione (10a) secondo una qualsiasi delle rivendicazioni precedenti, in cui detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi comprendono un valore di indirizzo temporaneo (TADR),

in cui detto aggiornare (2016) detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi al fine di indicare che l'indirizzo (ADR; MADR) estratto è sbloccato comprende di memorizzare detto indirizzo (ADR; MADR) estratto come detto valore di indirizzo temporaneo (TADR), e

in cui detto determinare (2004, 2006) se detti dati di configurazione (CFG; TADR, LSTAT) aggiuntivi indicano che l'indirizzo (ADR; MADR) estratto è bloccato o sbloccato comprende di confrontare detto indirizzo (ADR; MADR) estratto con detto valore di indirizzo temporaneo (TADR).

5. Sistema di elaborazione (10a) secondo una qualsiasi delle rivendicazioni precedenti, in cui detto circuito di interfaccia slave (1064a) è configurato per generare detto segnale di sblocco (UNLOCK; LOCK) confrontando uno o più bit di detto indirizzo (ADR; MADR) estratto con uno o più bit di detti dati (DATA; MDATA) estratti.

6. Sistema di elaborazione (10a) secondo la Rivendicazione 5, in cui detto circuito di interfaccia slave (1064a) è configurato per asserire detto segnale di sblocco (UNLOCK; LOCK) quando detto indirizzo (ADR; MADR) estratto corrisponde a detti dati (DATA; MDATA) estratti.

7. Sistema di elaborazione (10a) secondo una qualsiasi delle rivendicazioni precedenti, in cui il circuito comprende uno o più registri (1070) e uno o più circuiti periferici (1072) configurati per scambiare dati con detti uno o più registri (1070), e in cui un rispettivo dato indirizzo è associato a ciascuno di detti uno o più registri (1070) e detto circuito di interfaccia slave (1004a, 1024a, 1064a, 1104a) è configurato per inoltrare selettivamente dette richieste di scrittura (WREQ):

- determinando il registro (1070) associato all'indirizzo (ADR, MADR) estratto da detta richiesta di scrittura (WREQ), e

- memorizzando detti dati (DATA; MDATA) estratti da detta richiesta di scrittura (WREQ) nel rispettivo registro (1070).

8. Sistema di elaborazione (10a) secondo la Rivendicazione 7, in cui detto circuito di interfaccia slave (1064a) è un bridge periferico, in cui detti uno o più registri (1070) sono connessi a detto circuito di interfaccia slave (1064a) mediante un bus periferico (1074).

9. Sistema di elaborazione (10a) secondo la Rivendicazione 7 o la Rivendicazione 8, in cui detti dati di configurazione (1068) indicano per ciascuno di detti uno o più registri (1070) se il rispettivo indirizzo è protetto o non protetto.

10. Sistema di elaborazione (10a) secondo una qualsiasi delle rivendicazioni precedenti, in cui detto circuito di interfaccia slave (1064a) è configurato per:

- in risposta a una determinazione che l'indirizzo estratto (ADR; ADR) non è protetto o che l'indirizzo (ADR; MADR) estratto è sbloccato, inoltrare (2012) una risposta (SRESP) da detto circuito (100a, 102a, 106a, 110a) a detto sistema di comunicazione (114a);
- in risposta a una determinazione che l'indirizzo (ADR; MADR) estratto è protetto e che l'indirizzo (ADR; MADR) estratto è bloccato, e:
    - quando detto segnale di sblocco (UNLOCK; LOCK) è asserito, inviare (2016) una risposta (URESP) che indica che la richiesta di scrittura (WREQ) è stata eseguita, e

- quando detto segnale di sblocco (UNLOCK; LOCK) è deasserito, inviare (2010) una risposta (URESP) che indica che la richiesta di scrittura (WREQ) non è stata eseguita.

11. Circuito integrato comprendente un sistema di elaborazione (10a) secondo una qualsiasi delle rivendicazioni precedenti.

12. Dispositivo, come un veicolo, comprendente una pluralità di sistemi di elaborazione (10a) secondo una qualsiasi delle Rivendicazioni precedenti da 1 a 10, in cui detti sistemi di elaborazione (10a) sono connessi mediante un ulteriore sistema di comunicazione (20).

13. Procedimento di funzionamento di un sistema di elaborazione (10a) secondo una qualsiasi delle rivendicazioni precedenti da 1 a 10, comprendente:

- fornire dati di configurazione (1068; EN, P) a detto circuito di interfaccia slave (1064a), in cui detti dati di configurazione (1068; EN, P) indicano che detto dato indirizzo è protetto;

- inviare una prima richiesta di scrittura (WREQ) a detto sistema di comunicazione (114a), detta prima richiesta di scrittura (WREQ) comprendendo detto dato indirizzo e dati (DATA; MDATA) determinati in funzione di detta regola predeterminata in funzione di detto dato indirizzo; e

- inviare una seconda richiesta di scrittura (WREQ) a detto sistema di comunicazione (114a), detta seconda richiesta di scrittura (WREQ) comprendendo detto dato indirizzo e dati (DATA; MDATA) da scrivere in detto dato indirizzo.

FIG. 1

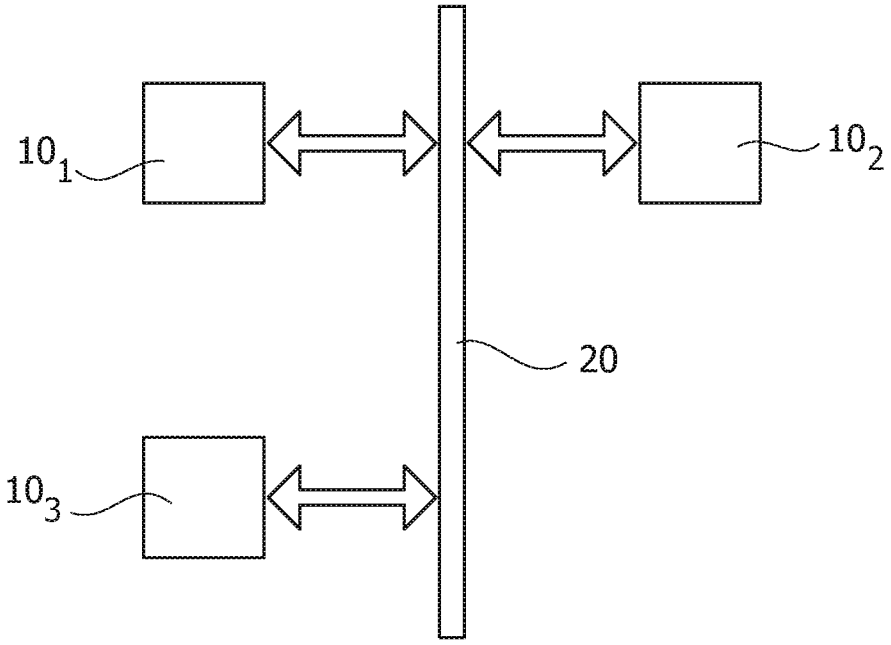


FIG. 2

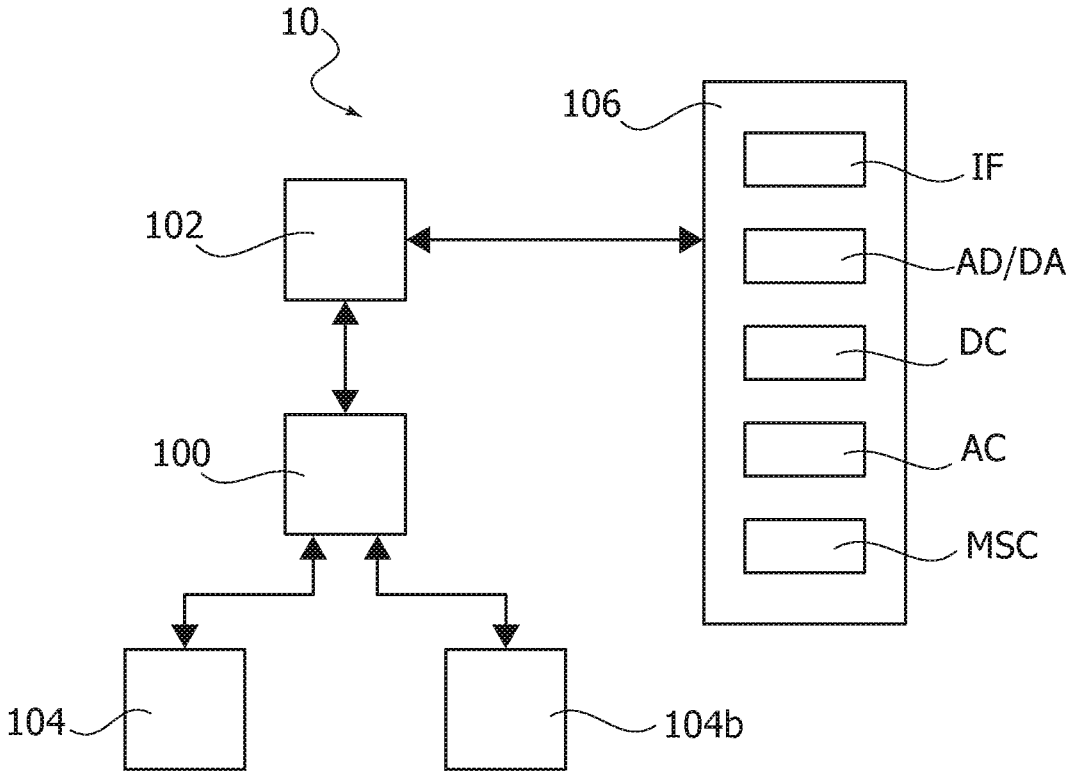


FIG. 3

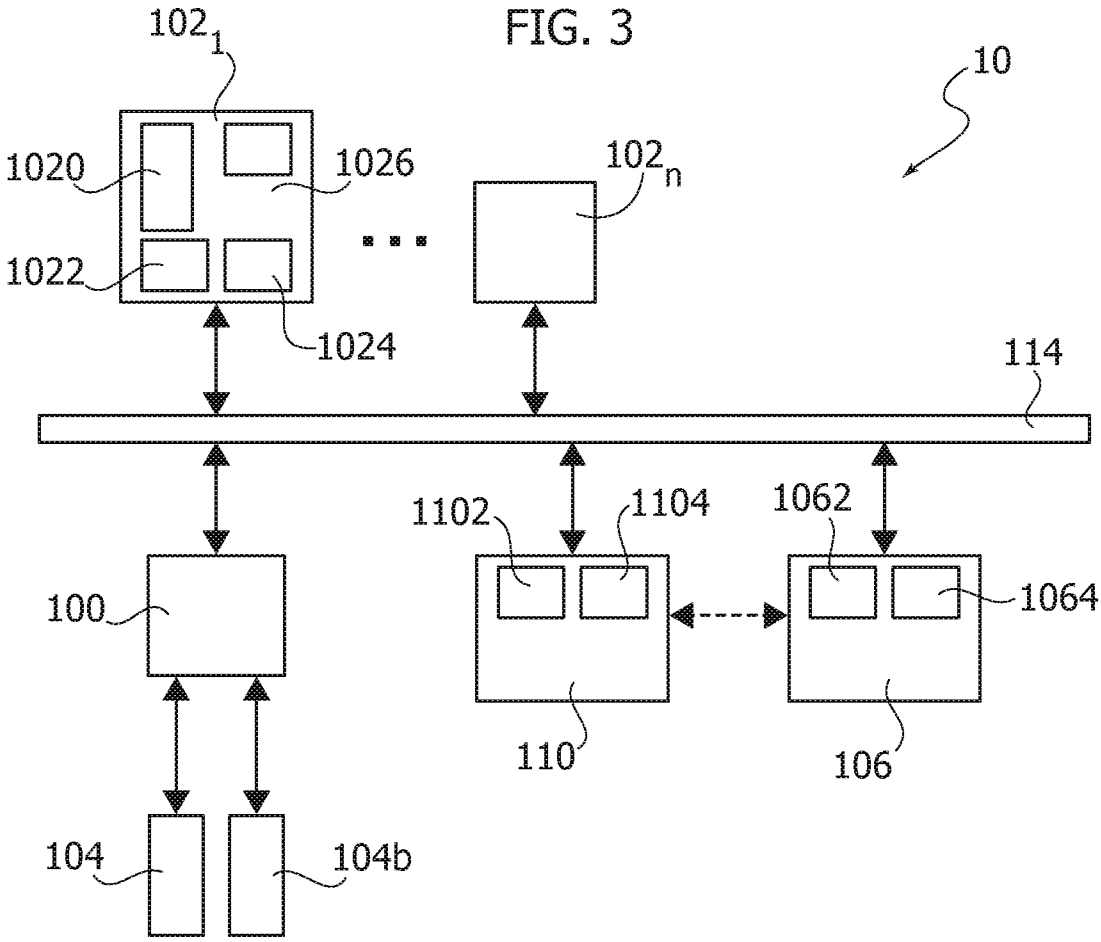

102 1
10
1020
1026
102 n
1022
1024
114
1102
1104
1062
100
1064
110
106
104
104b

FIG. 4

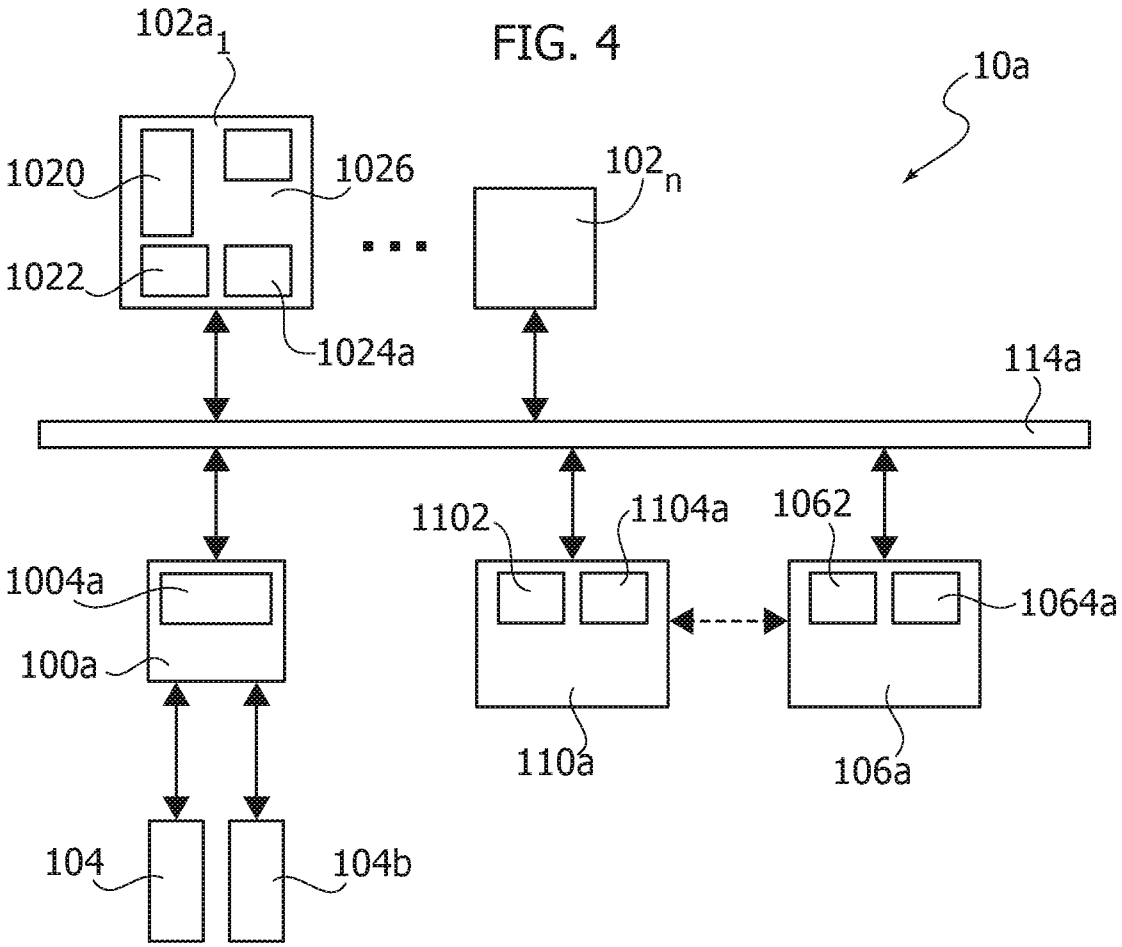

102a 1
10a
1020
1026
102 n
1022
1024a
114a
1102
1104a
1062
1004a
1064a
100a
110a
106a
104
104b

FIG. 5

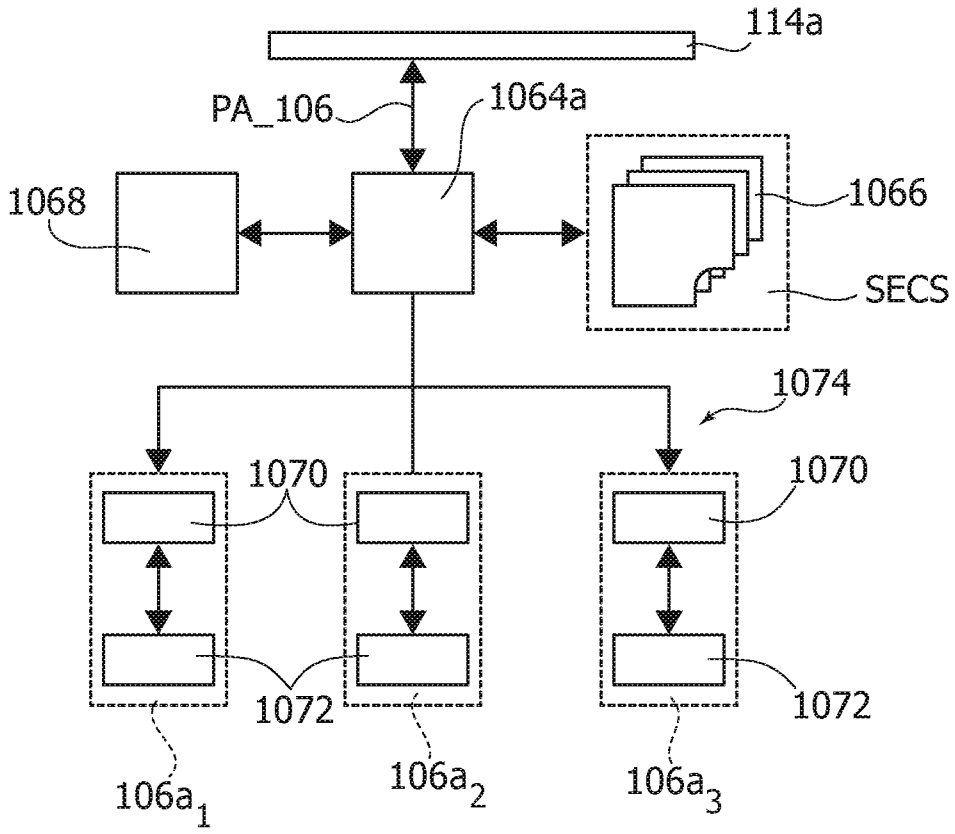

114a
PA_106
1064a
1068
1066
SECS
1074
1070
1070
1072
1072
106a1
106a2
106a3

FIG. 6

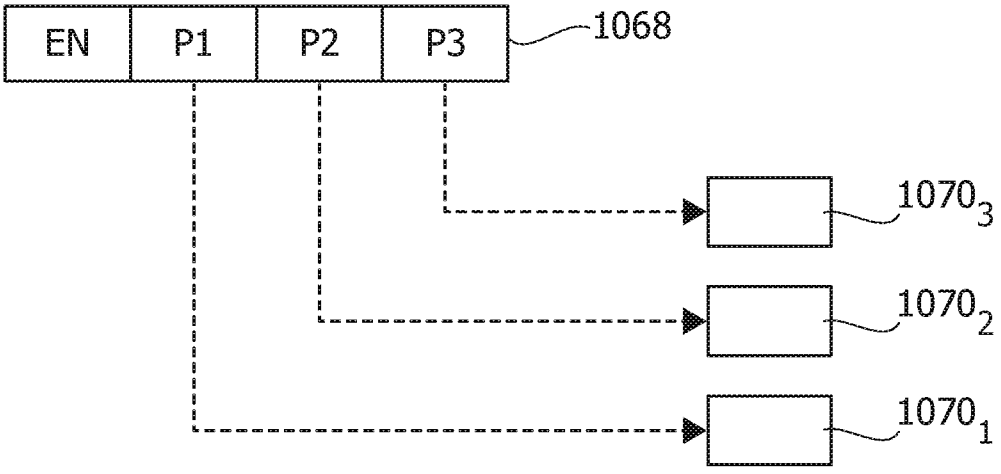

EN
P1
P2
P3
1068
1070_3
1070_2
1070_1

FIG. 7

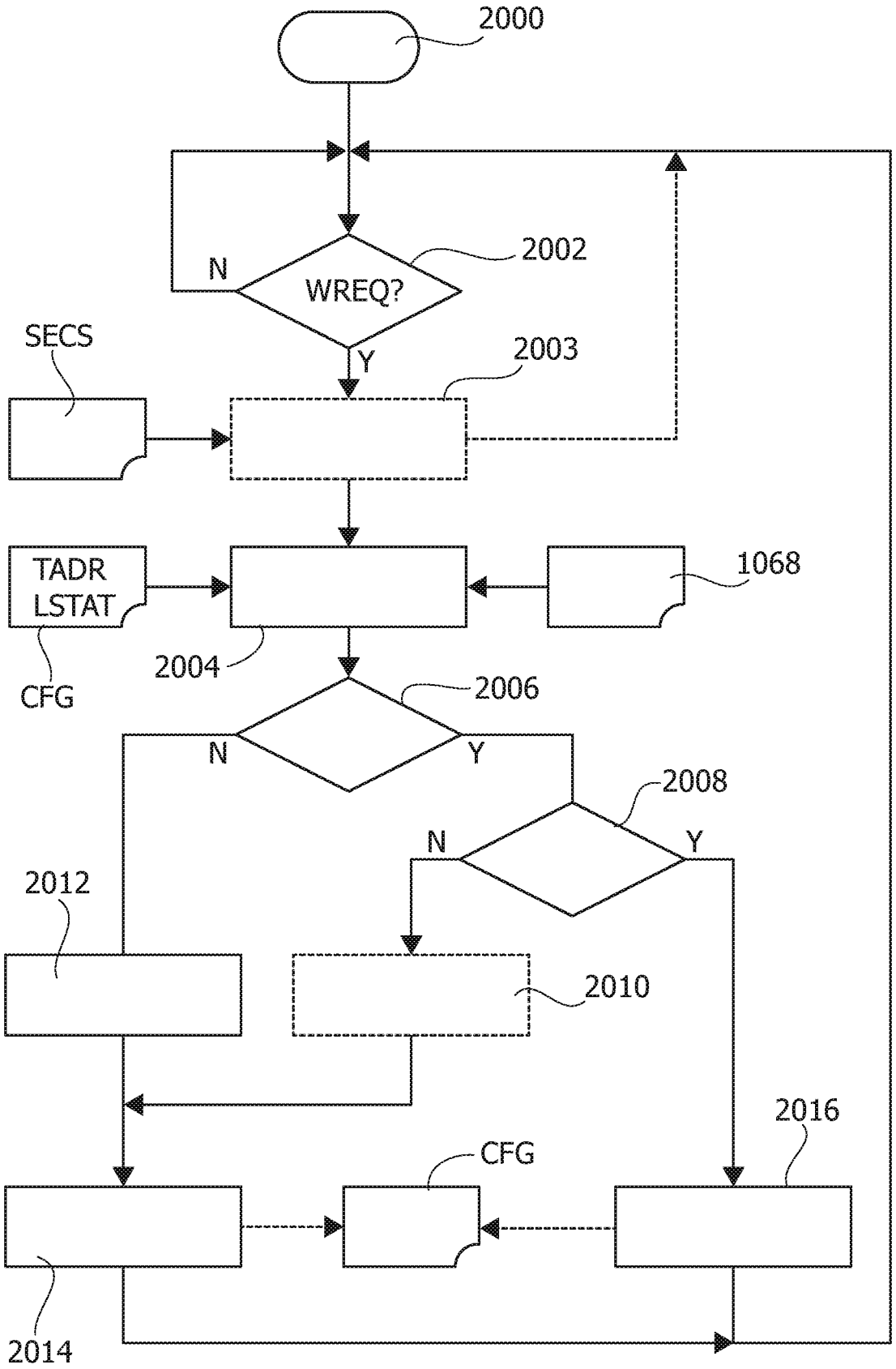

2000
2002
N
WREQ?
Y
SECS
2003
TADR
LSTAT
1068
CFG
2004
2006
N
Y
2008
N
Y
2012
2010
2016
CFG
2014

FIG. 8

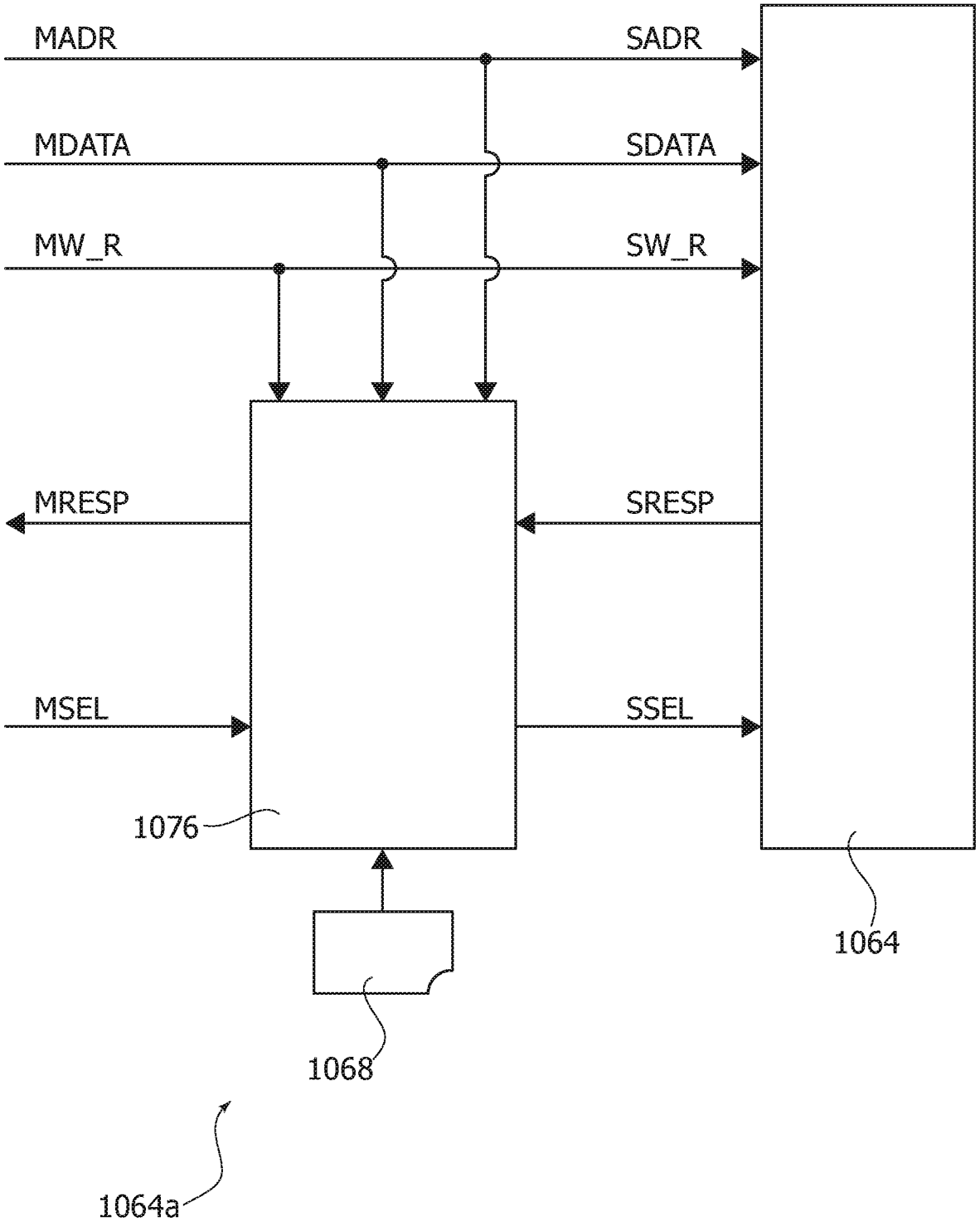
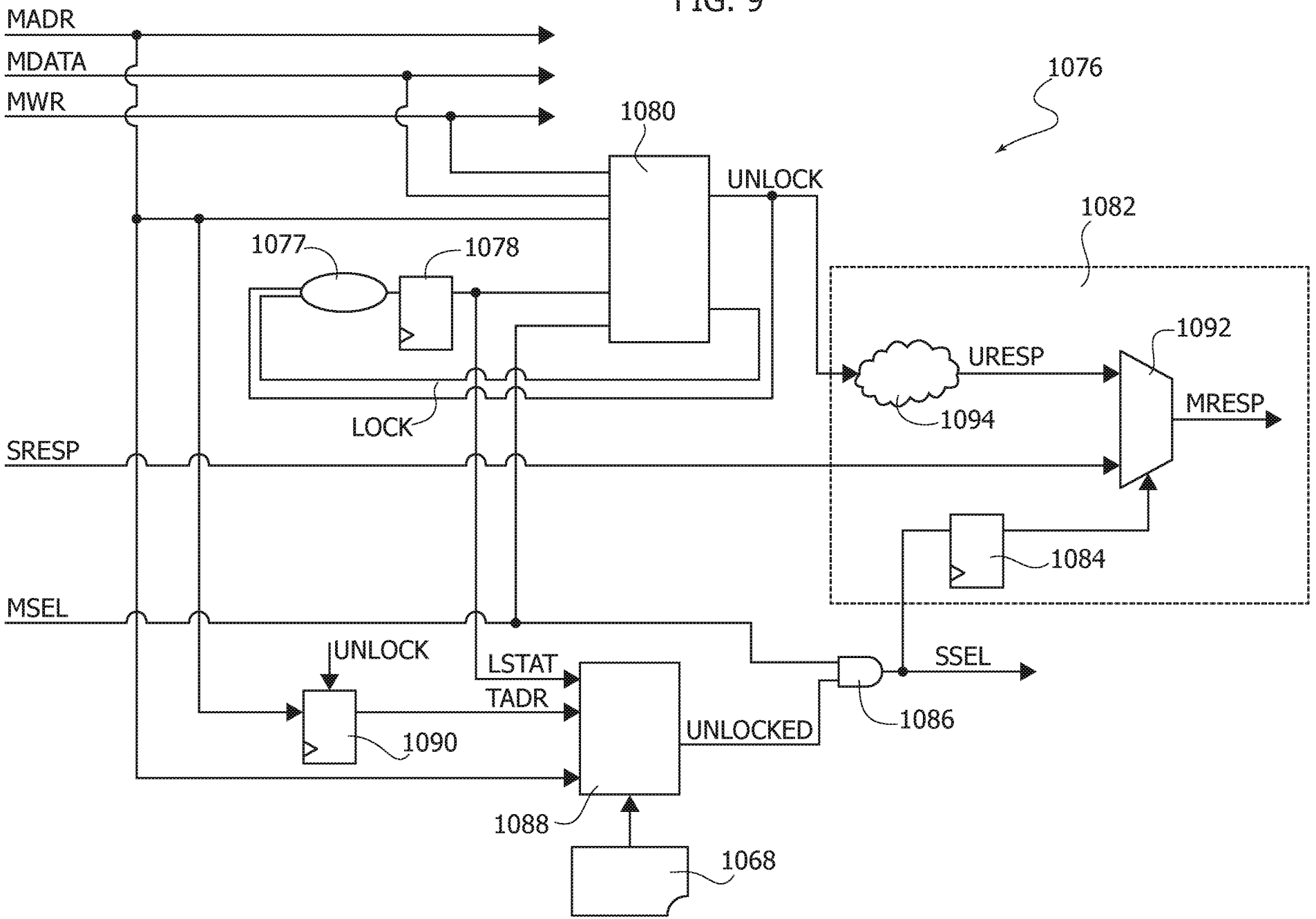

MADR
SADR
MDATA
SDATA
MW_R
SW_R
MRESP
SRESP
MSEL
SSEL
1076
1064
1068
1064a

FIG. 9


MADR
MDATA
MWR
1076
1080
UNLOCK
1082
1077
1078
1092
URESP
MRESP
1094
LOCK
SRESP
1084
MSEL
UNLOCK
LSTAT
TADR
SSEL
1086
1090
UNLOCKED
1088
1068