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

UIBM

DOMANDA DI INVENZIONE NUMERO	**102021000021944**
Data Deposito	**17/08/2021**
Data Pubblicazione	**17/02/2023**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	74

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	79

Titolo

Schermatura di registri in dispositivi a semiconduttore

DESCRIZIONE dell'invenzione industriale dal titolo:
"Schermatura di registri in dispositivi a semiconduttore"
di: STMicroelectronics S.r.l., di nazionalità italiana, via C. Olivetti, 2 - 20864 Agrate Brianza (MB) - Italia
Inventori designati: Salvatore Marco ROSSELLI, Giuseppe GUARNACCIA
Depositata il: 17 agosto 2021

****

TESTO DELLA DESCRIZIONE

Campo tecnico

La descrizione è relativa ai dispositivi a semiconduttore.

Una o più forme di attuazione possono essere applicate a una varietà di prodotti come, per esempio, i microcontrollori o i microprocessori.

Sfondo

Un SoC (System on Chip) digitale, come un microprocessore o un microcontrollore non specializzato (GP, "General Purpose") comprende un grande insieme di core IP (IP) digitali.

La designazione core IP ("Intellectual Property" ossia proprietà intellettuale) - in breve, core IP o semplicemente IP - si applica a un blocco di logica o di dati che può essere usato nel produrre un circuito, come una FPGA (Field Programmable Gate Array) o un ASIC (Application Specific Integrated Circuit) per un prodotto.

Gli IP possono essere molto complessi e supportare molte caratteristiche.

Certi IP possono essere progettati per funzionare soltanto in particolari contesti e possono diventare inutili, o perfino dannosi, in altri contesti. Per esempio, un IP progettata per un microcontrollore (MCU, "MicroController Unit") può non essere adatto per un microprocessore (MPU, "MicroProcessor Unit") e/o un IP progettato per un certo cliente può non essere compatibile per l'uso con un firmware vecchio, e così via.

Si potrebbe considerare di affrontare questi problemi impedendo fisicamente che alcuni registri siano istanziati in un progetto di un certo dispositivo. Tuttavia, possono insorgere situazioni in cui "il silicio è già fuori" ("out"): per esempio, il relativo dispositivo è già in produzione, cosicché è semplicemente troppo tardi per implementare un tale intervento. Sarebbe vantaggioso potere disabilitare/impedire selettivamente caratteristiche di funzionamento indesiderate o "bacate" ("buggy") senza riprogettare un circuito.

Scopo e sintesi

Una o più forme di attuazione contribuiscono a fornire una tale capacità vantaggiosa tramite un dispositivo a semiconduttore come esposto nelle rivendicazioni che seguono.

Un System on Chip (SoC) può essere un esempio di un dispositivo a semiconduttore in cui le forme di attuazione possono essere applicate in modo vantaggioso.

Una o più forme di attuazione sono relative a un procedimento corrispondente.

Le rivendicazioni sono parte integrante dell'insegnamento tecnico qui fornito con riferimento alle forme di attuazione.

Una o più forme di attuazione forniscono un meccanismo "post-silicio" per rendere sicuri i campi e i registri dell'IP.

Una o più forme di attuazione definiscono una caratteristica di abilitazione/disabilitazione all'interno dei componenti di decodifica/indirizzamento/bridging di un percorso di dati ("datapath") di registri.

Una o più forme di attuazione possono essere usate per proteggere/bloccare in un contesto sicuro caratteristiche non sicure.

Una o più forme di attuazione possono basarsi su celle programmabili una volta sola od OTP ("One Time Programmable"). Queste celle possono essere rese disponibili o sono già disponibili in un SoC in varie forme (come, per esempio, fusibili elettronici). Queste celle possono essere programmate al momento della produzione per impostare i componenti (per es., i componenti di decodifica, indirizzamento e/o bridging) di un percorso dati di registro. In tal modo, gli accessi ai registri possono essere controllati (per es., abilitati selettivamente/mascherati in scrittura/negati) selettivamente, con una granularità regolabile in modo fine.

Una o più forme di attuazione facilitano la protezione (schermatura) di caratteristiche che non si intende/desidera esporre pubblicamente. Può essere così in quanto tali caratteristiche danno origine a problemi legacy e/o corrispondono a errori identificati e corretti oppure a causa di motivi legali, come un controllo sull'esportazione, tali da indicare che una caratteristica sviluppata per un cliente non sarà disponibile per il mercato di massa.

Analogamente, si può desiderare che lacune nella sicurezza (per es., bachi ("bug") trovati nel silicio e a cui si è rimediato) e/o caratteristiche suscettibili di essere considerate come caratteristiche non a specifica, vecchie e/o legacy oppure caratteristiche progettate per uno scopo differente siano escluse da una esposizione al mercato di massa.

Una o più forme di attuazione facilitano il fatto di evitare tale esposizione indesiderata/involontaria.

In una o più forme di attuazione, si può metter in atto un rimedio adeguato senza l'intervento di un team di progettazione ("design team") per un nuovo tape-out o una riprogettazione del sistema, per esempio.

Breve descrizione delle figure annesse

Una o più forme di attuazione saranno descritte ora, a puro titolo di esempio non limitativo, con riferimento alle figure annesse, nelle quali:

la Figura 1 è un esempio di uno schema a blocchi di un contesto in cui le forme di attuazione possono essere applicate vantaggiosamente;

la Figura 2 è un esempio di uno schema funzionale di possibili implementazioni di forme di attuazione della presente descrizione;

la Figura 3 è un esempio di uno schema a blocchi di possibili implementazioni di forme di attuazione della presente descrizione;

la Figura 4 è un esempio di uno schema di una possibile applicazione di forme di attuazione della presente descrizione;

le Figure 5, 6 e 7 sono esempi di possibili dettagli di implementazione di forme di attuazione della presente descrizione; e

la Figura 8 è un esempio di uno schema a blocchi di un possibile contesto di uso di forme di attuazione.

I simboli e i numeri corrispondenti nelle differenti figure si riferiscono in generale a parti corrispondenti a meno che sia indicato altrimenti.

Le figure sono disegnate per illustrare chiaramente gli aspetti rilevanti delle forme di attuazione e non sono disegnate necessariamente in scala.

I bordi di caratteristiche disegnate nelle figure non indicano necessariamente il termine dell'estensione della caratteristica.

Descrizione dettagliata

Nella descrizione che segue sono illustrati vari dettagli specifici, allo scopo di fornire una comprensione approfondita di vari esempi di forme di attuazione secondo la descrizione. Le forme di attuazione possono essere ottenute senza uno o più dei dettagli specifici o con altri procedimenti, componenti, materiali, ecc. In altri casi, operazioni, materiali o strutture note non sono illustrate o descritte in dettaglio in modo tale da non rendere poco chiari vari aspetti delle forme di attuazione.

Un riferimento a "una forma di attuazione" nel quadro della presente 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. Per cui, le frasi come "in una forma di attuazione" o simili che possono essere presenti in vari punti della presente

descrizione non fanno necessariamente riferimento esattamente proprio 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 comodità e quindi non definiscono l'ambito di protezione o l'ambito delle forme di attuazione.

Come discusso nella parte introduttiva di questa descrizione, un SoC (System on Chip) digitale, quale un microprocessore o un microcontrollore non specializzato (GP), comprende un grande insieme di core IP (IP) digitali. Gli IP possono essere molto complessi e possono supportare molte caratteristiche.

Certi IP possono essere progettati per funzionare soltanto in particolari contesti e possono diventare inutili, o perfino dannosi, in altri contesti.

Per esempio, e puramente a titolo di esempio:

un IP progettato per un microcontrollore (MCU) può non essere adatto per un microprocessore (MPU),

un IP progettato per un certo cliente può non essere compatibile per l'uso con un firmware vecchio, e/o

può essere previsto che certe caratteristiche adottate in un firmware vecchio siano abbandonate (discontinuate) in un firmware nuovo.

Nella Figura 1 è rappresentato un dispositivo a semiconduttore 1 quale un system-on-chip (SoC) - non visibile nella sua interezza - comprendente una porzione 10 (per esempio, un IP comprendente una periferica sicura) accoppiata a una rete di interconnessione ICN.

Come illustrata, la porzione di dispositivo 10 comprende uno o più registri 12. Questi possono essere, per

esempio, registri sicuri che ci si aspetta siano usati nel funzionamento corrente del dispositivo.

Inoltre, il dispositivo 1 può avere caricato in esso in un vecchio registro non protetto 14 del codice "legacy". Questo codice può finire col diventare inutile o perfino dannoso: per esempio, può alterare la "endianness", che è l'ordine o la sequenza dei byte di una parola di dati digitali in una memoria.

A titolo di esempio, si può ipotizzare essere previsto che la periferica 10 della Figura 1 si interfacci tramite un'interfaccia IF con una memoria esterna sicura 16 che ha memorizzati in essa record sicuri 18 (indicati per semplicità con ABCDEFGH).

In una situazione come illustrata nella Figura 1, hackerare l'endianness può avere come risultato il fatto che vengano corrotti record sicuri dell'utente (ABCDEFGH >>> ABCDHGFE).

Una situazione come illustrata nella Figura 1 può sorgere, per esempio, in circostanze in cui:

una caratteristica per rimappare l'interfaccia IF esterna verso una memoria 16 è stata progettata e testata anni addietro sulla periferica 10, con tale caratteristica successivamente esclusa dalla specifica ma mantenuta, per qualche motivo, in un core IP come codice legacy (memorizzato in un registro, come 14), e

il controllore è stato selezionato per un nuovo SoC, che integra nuove caratteristiche di sicurezza con una specifica di sicurezza che non ha considerato la presenza del codice legacy (rimanente).

I team di progetto e di verifica coinvolti nel progetto del nuovo SoC possono notare la presenza di questo

codice legacy e adottare misure per renderlo sicuro, anche se non stabilito nella specifica.

La presenza del codice legacy (non più specificato) può tuttavia passare inosservata con possibili effetti negativi come discusso in precedenza (un vecchio registro non protetto, una possibile alterazione dell'endianness e di record sicuri dell'utente corrotti).

Il fatto che la presenza del codice legacy (non più specificato) passi inosservato può essere dovuto a vari fattori, per es.:

la complessità del sistema, con la complessità che produce errori; e/o

il codice legacy è relativo a caratteristiche che non sono di interesse per l'utente del nuovo sistema: con riferimento all'esempio della Figura 1, la caratteristica di rimappatura del software può essere completamente sconosciuta al nuovo cliente, che è preoccupato principalmente della sicurezza dei dati.

Queste caratteristiche "inutili" che rimangono nel sistema possono tuttavia avere un impatto su caratteristiche che contano davvero.

Inoltre, alcuni possibili errori possono essere particolarmente infelici e possono richiedere un tape-out completamente nuovo.

D'altra parte, come indicato, in certe circostanze (per es., con un silicio già "rilasciato", vale a dire, con il dispositivo a semiconduttore corrispondente già in produzione) è semplicemente troppo tardi implementare un tale intervento.

La Figura 1 reppresenta così un esempio generale di un contesto in cui le forme di attuazione possono essere applicate vantaggiosamente, cioè un dispositivo a

semiconduttore 1 (per esempio, un SoC, come un microcontrollore, MCU o un microprocessore, MPU) comprendente registri 12 e 14 configurati per avere segnali digitali memorizzati in essi.

Come illustrato, il dispositivo a semiconduttore 1 è configurato (tramite l'interfaccia IF, per esempio) per la comunicazione con almeno un ulteriore dispositivo 16 (una memoria sicura esterna, per esempio).

Per esempio, come discusso in precedenza, i registri 12 possono essere registri sicuri da usare per il funzionamento previsto corrente del dispositivo o al contrario registri vecchi, non protetti, che hanno caricato in essi un codice "legacy" che è inutile o perfino fastidioso.

Durante la comunicazione del dispositivo a semiconduttore 1 con l'ulteriore dispositivo o gli ulteriori dispositivi 16, il registro o i registri 14 può (possono) così essere esposto (esposti) a richieste di accesso.

La Figura 2 è un esempio di uno schema funzionale di possibili forme di attuazione che comportano l'uso di uno o più schermi di registro 100 per schermare istanze di una periferica 10 (per es., registri quali i registri 14 in essa compresi come rappresentato a titolo di esempio nella Figura 1) rispetto a tali richieste di accesso.

Come discusso ulteriormente in seguito, il circuito o i circuiti di schermo di registro 100 accoppiato (accoppiati) al registro o ai registri 14 comprende (comprendono) una circuiteria di rilevazione di accesso 200 (si vedano le Figure da 5 a 7) configurata per rilevare le richieste di accesso per l'accesso al registro (ai

registri) 14 durante la comunicazione del dispositivo a semiconduttore 1 con il dispositivo o i dispositivi 16.

La circuiteria di schermo di registro 100 è configurata per essere attivata selettivamente in una modalità di funzionamento di schermo di registro per schermare (completamente) il registro (i registri) 14 da queste richieste di accesso.

Quando attivata nella modalità di schermo di registro, la circuiteria di schermo di registro 100 impedisce l'accesso al registro o ai registri 14 in risposta alle richieste di accesso rilevate dalla circuiteria di rilevazione di accesso.

Negli esempi qui discussi, lo schermo (gli schermi) di registro 100 coopera (cooperano) con celle OTP (programmabili una volta sola) 102 con caratteristiche di abilitazione di cella OTP 104 associate.

Agli esperti nella tecnica è nota attualmente una varietà di implementazioni di OTP tradizionali che possono essere applicate vantaggiosamente in esempi come qui presentato. Questi esempi sono in effetti in gran parte "trasparenti" rispetto alle specifiche implementazioni di OTP usate.

La Figura 3 è un esempio di uno schema a blocchi di possibili dettagli di implementazione di forme di attuazione della presente descrizione.

Come illustrato nella Figura 3, uno schermo di registro 100 può essere implementato come una parte di un componente digitale attivo, quale un'interfaccia digitale (per es., un'interconnessione, come le interfacce AMBA, Advanced Microcontroller Bus Architecture, o dispositivi ponte ("bridge") di protocollo) in un sistema comprendente

una circuiteria logica centralizzata in una matrice di bus/interconnessione e/o in bridge di protocollo.

Un sistema come illustrato nella Figura 3 comprende una unità di elaborazione (una CPU, per esempio) 106 con associata una circuiteria di accesso diretto in memoria (DMA, "Direct Memory Access") 108 accoppiata tramite una matrice di bus/interconnessione 110 ed, eventualmente, un bridge di protocollo 112, a varie istanze di periferica - come rappresentato dal riferimento 10 nella Figura 2.

Queste istanze di periferica possono comprendere (puramente a titolo di esempio):

un'interfaccia di memoria non volatile 10A,

un'interfaccia di controllo di memoria ad accesso casuale (RAM, "Random-Access-Memory") 10B,

un'interfaccia di memoria esterna 10C,

un'interfaccia di periferica seriale (SPI, "Serial Peripheral Interface") 10D, e

un bus seriale universale (USB, "Universal Serial Bus") 10E.

Come rappresentato a titolo di esempio nella Figura 3, la comunicazione con le istanze di periferica 10A, 10B e 10C avviene tramite la matrice di bus/interconnessione 110 (con gli schermi di registri 100 che rappresentano particolari interfacce target o nodi di interconnessione/bus 100A, per esempio) e la comunicazione con le istanze di periferica 10D e 10E coinvolge il bridge di protocollo 112.

Come illustrato, ciascuno schermo di registro 100 ha associato a esso un insieme di celle OTP, indicate collettivamente come 102 nella Figura 3.

Queste celle possono essere implementate, in base alle specifiche del SoC, come opzioni di metallo di fusibili

elettronici (e-fuse, "electronic fuse"), celle proprietarie, bit di opzione in una memoria non volatile (NVM, "Non-Volatile Memory") e così via, come d'altronde tradizionale nella tecnica.

In pratica, gli schermi di registro 100 possono essere considerati come degli switch di abilitazione ("enable") e un insieme di indirizzi di registri "proibiti". Quando un tale switch è in ON (conduttivo) e si rileva un accesso in scrittura verso uno dei registri proibiti, l'accesso è filtrato via in modo tale che i dati nei registri, come 14, non siano esposti (come si può desiderare per vari motivi, come discusso in precedenza).

Gli schermi di registro 100 possono essere implementati come una caratteristica in un'interfaccia target o in un nodo di interconnessione esistente.

La Figura 4 si riferisce a titolo di esempio a un sistema comprendente N istanze di periferica da 10_1 a 10_N, comprendenti ciascuna due registri, un Registro 1 e un Registro 2, per esempio. La barra RB rappresenta i bit dei registri che sono protetti.

Vengono usati N fusibili elettronici (e-fuse) - 20 o 30 è stato riscontraro essere un numero adeguato - per la selezione (Periferica/Registro/nibble) a scopi di mascheratura.

Per esempio (questi dati quantitativi sono puramente a titolo di esempio e non sono limitativi):

cinque bit selezioneranno la periferica (per es.: la periferica 10_2);

dieci bit selezioneranno il registro (per es.: il Registro 2);

una maschera di 8 bit selezionerà un nibble di 4 bit da proteggere (bit 23:20, per esempio); e

la maschera può essere applicata a una pluralità di campi o al registro completo.

Le Figure 5, 6 e 7 illustrano uno schermo di registro 100 come rappresentato qui a titolo di esempio, implementato come un modulo autonomo ("stand-alone") dedicato di un'interconnesione (cioè: un bus APB, Advanced Peripheral Bus, o un bus AHB, Advanced High-performance Bus) comprendente un decodificatore di indirizzi 200 accoppiato, per esempio, a un bus e-fuse 20/30 e a un generatore di risposte 201.

Un tale modulo può fornire un messaggio di errore o una risposta finta quando si verifica la concordanza ("match") con un indirizzo protetto (vale a dire, quando si tenta di accedere a un registro "proibito" 14).

Un tale modulo può essere implementato come un sotto-modulo di un decodificatore o un bridge di interconnessione (da AHB ad APB, per esempio).

Nelle Figure 5 e 6 sono illustrate due possibili implementazioni.

La Figura 5 illustra una possibile implementazione come componente autonomo, costituito da una logica di decodifica (il decodificatore di indirizzi 200, avente eventualmente associata a esso una logica di filtraggio) e da un generatore di risposte 201.

La Figura 6 illustra una possibile implementazione in cui il decodificatore di indirizzi 200 e il generatore di risposte 201 sono sotto-blocchi comuni di componenti di interconnessione (come un bridge di protocollo). Integrando il blocco circuitale di filtraggio (indicato espressamente come 200A) per lo schermo di registro in uno stesso componente del decodificatore di indirizzi 200 (esistente),

una tale implementazione facilita il risparmio di area e la riduzione di complessità.

La Figura 7 (che si riferisce all'implementazione della Figura 5) illustra il decodificatore di indirizzi 200 accoppiato a un ingresso 202 con il bus di OTP (si veda anche 102 nella Figura 3). Ciò può essere tramite un controllore digitale dedicato per la gestione di OTP, che facilita la programmazione e la lettura delle celle OTP secondo vincoli di sicurezza o tramite dei bit di opzione.

Il decodificatore di indirizzi 200 può essere configurato per rilevare le richieste (indicate come 204) di accesso a un registro "proibito" come ricevute sul bus di richieste AHB.

La reazione dello schermo di registro può essere:

un messaggio di errore generato nel modulo di generazione di risposte 201, o

lo schermo 100 che rimane silenzioso.

L'opzione adottata può essere funzione dei contenuti di un registro di configurazione 208 accoppiato al bus di OTP (bus e-fuse).

Il messaggio di errore può essere inviato all'indietro sul bus di risposte AHB in risposta al fatto che da parte del decodificatore di indirizzi 20 viene rilevata una richiesta 204 di accesso a un registro "proibito".

Questo può avvenire tramite un multiplexer 210 controllato dal decodificatore di indirizzi 200, il multiplexer 210 avendo un primo ingresso accoppiato al modulo di generazione di risposte 201 e un secondo ingresso accoppiato alla porta di ingresso del bus di risposte AHB allo schermo 100.

Un'interruzione ("interrupt")/uscita di accesso erroneo può esser usata per allertare il sistema di

sicurezza o per abilitare selettivamente ("gate") informazioni di sicurezza.

Le Figure 5 e 6 più la Figura 7, come sono ad ora discusse, sono pertanto illustrative di un dispositivo a semiconduttore 1 comprendente una o più porzioni di registro (sebbene per semplicità si sia fatto qui riferimento a un intero registro 14, la discussione si applica in modo identica anche solo a una porzione di un registro) configurate per avere segnali digitali memorizzati in esse.

Il dispositivo a semiconduttore 1 è configurato (si vedano, per esempio, i riferimenti IF; 110, 112; da 10A a 10E) per la comunicazione con almeno un ulteriore dispositivo 16 all'esterno del dispositivo 1. Durante la comunicazione del dispositivo a semiconduttore 1 con il dispositivo 16, una certa porzione o certe porzioni di registro "proibita"/"proibite" o "indesiderata"/"indesiderate" 14 è esposta/sono esposte a richieste di accesso.

Come discusso, la circuiteria di schermo di registro 100 comprende una circuiteria di rilevazione di accesso 200 configurata per rilevare le richieste di accesso per accedere a questo registro (questi registri) 14 durante la comunicazione del dispositivo a semiconduttore 1 con il dispositivo 16.

La circuiteria di schermo di registro 100 è configurata per essere attivata selettivamente, per es., tramite il registro di configurazione 208 (sensibile alle informazioni di configurazione come ricevute, per es., tramite il bus di OTP) in una modalità di schermo di registro.

Quando attivata nella modalità di schermo di registro, la circuiteria di schermo di registro 100 impedisce l'accesso alle porzioni di registro 14 in risposta alle richieste di accesso rilevate dalla circuiteria di rilevazione di accesso 200.

Un dispositivo come illustrato nelle Figure 5 e 6 più la Figura 7, come discussa fino a ora, si presta a identificare una o più porzioni di registro 14 nel dispositivo a semiconduttore 1 configurate per avere memorizzati in esse segnali digitali previsti per essere esclusi dalla comunicazione con il dispositivo 16. Questo può essere il caso, per esempio, di segnali digitali corrispondenti a una caratteristica sviluppata (esclusivamente) per un cliente e/o a caratteristiche che non destante a essere esposte al mercato di massa per motivi legali.

La circuiteria di schermo di registro 100 accoppiata alle porzioni di registro 14 così identificate può essere attivata (secondo il controllo di OTP, per esempio, come rappresentato a titolo di esempio dal riferimento 102) nella modalità di schermo di registro.

Quando attivata nella modalità di schermo di registro, la circuiteria di schermo di registro 100 scherma (completamente) dalle richieste di accesso le porzioni di registro 14 identificate, per es., impedendo l'accesso in risposta alle richieste di accesso a essa come rilevato dalla circuiteria di rilevazione di accesso 200.

Vantaggiosamente, come illustrato nella Figura 7, può essere previsto un ulteriore multiplexer 212 controllato dal registro di configurazione 208.

L'ulteriore multiplexer 212 ha la sua uscita accoppiata alla porta di uscita del bus di richieste AHB.

Inoltre, l'ulteriore multiplexer 212 ha un primo ingresso accoppiato a un bus dati DB (si può ipotizzare che questo sia dalle porzioni di registro 14 "critiche") nello schermo 100 e un secondo ingresso accoppiato a un blocco di inversione 214 che può essere usato per invertire specifici bit di dati sul bus DB secondo il controllo del registro di configurazione 208.

In base alle informazioni lette sul bus di OTP fornite al registro di configurazione 208 tramite un rilevatore di inversione 214A, il blocco di inversione 214 può essere controllato dal registro di configurazione 208 al fine di invertire certi bit nei dati ricevuti sul bus di dati DB.

La caratteristica di inversione appena discussa consente di configurare la circuiteria di schermo di registro 100 (sotto il controllo del registro di configurazione 208, che riceve a sua volta informazioni corrispondenti sul bus di OTP) in una modalità di mascheratura di registro, vale a dire, una sorta di modalità di "schermo bucato".

Quando attivata nella modalità di mascheratura di registro, la circuiteria di schermo di registro 100 consente di per sè un accesso alle porzioni di registro 14 in risposta alle richieste di accesso a essa come rilevato dalla circuiteria di rilevazione di accesso 200.

In tal caso, tuttavia, la circuiteria di schermo di registro "bucato" applica (tramite il blocco di inversione 214) una configurazione ("pattern") di mascheratura dei bit sui dati restituiti dalle porzioni di registro 14, sul bus DB, in risposta alle richieste di accesso.

Come rappresentato qui a titolo di esempio, una tale configurazione di mascheratura di bit comprende una inversione logica di bit selezionati (identificati, per

es., tramite informazioni fornite sul bus di OTP) nei dati restituiti sul bus DB dalle porzioni di registro 14 in risposta alle richieste di accesso ammesse dallo schermo "bucato".

Un dispositivo come illustrato nella Figura 7 e comprendente una tale caratteristica vantaggiosa di modalità di mascherature si presta a identificare (ulteriori) porzioni di registro 14 configurate per avere memorizzati in esse segnali digitali previsti per avere applicata una configurazione di mascheratura di bit (per es., nel blocco di inversione 214) nella comunicazione con il dispositivo 16.

Questo può essere il caso, per esempio, di dati affetti da un errore di implementazione di uno o più bit (considerati con una polarità erronea, per esempio).

In tal caso, non sussiste di per sè alcuna necessità di impedire un'esposizione dei dati (per es., nella loro interezza). La caratteristica vantaggiosa di modalità di mascheratura facilita tuttavia un funzionamento "fissato".

Il fatto di attivare (per es., tramite il controllo di OTP come rappresentato a titolo di esempio in 102) la circuiteria di schermo di registro 100 nella modalità di mascheratura di registro ha come risultato che la circuiteria di schermo di registro 100 diventa "bucata" (leaky) e consente un accesso alle ulteriori porzioni di registro 14 identificate.

Quando nella modalità di mascheratura di registro, la circuiteria di schermo di registro 100 applica una configurazione di mascheratura di bit (per es., tramite il blocco di inversione 214) ai dati restituiti (per es., sopra il bus DB) dalle (ulteriori) porzioni di registro 14

identificate in risposta alle richieste di accesso che sono state ammesse.

Questo può essere controllato tramite il contenuto del registro di configurazione 208, che è il risultato dell'elaborazione dei valori di OTP come indicato dal bus di OTP.

Come illustrato nella Figura 7, un registro di stato 216 memorizza informazioni e dettagli circa gli accessi tentati/concessi ed emette corrispondenti messaggi wrong_access_irq.

La Figura 8 mostra, con un confronto diretto con la Figura 1 (elementi o parti corrispondenti sono indicati con simboli di riferimento corrispondenti in entrambe le figure), che il comportamento dello (di ciascuno) schermo di registro 100 è determinato staticamente e strutturalmente dalle celle OTP 102. Queste possono essere fornite direttamente sul die finale.

Per esempio, in presenza di un codice "legacy" in un vecchio registro non protetto 14 (che può produrre indesideratamente dati corrotti) oppure si riscontra esitere qualche vulnerabilità nel SoC 10, la situazione può essere rimediata - senza l'intervento di una team di progettazione per un nuovo tape-out o per riprogettare il sistema - schermando semplicemente un qualsiasi registro "indesiderato", come il registro 14.

In tal modo, anche se presente "fisicamente", questo registro può essere considerato alla fine come inesistente a causa dell'azione di schermatura dello schermo 100.

Come discusso con riferimento alla Figura 7, certi esempi possono comprendere una caratteristica vantaggiosa di "schermo bucato" (leaky). In tal modo, un'operazione che implica una azione di schermatura assoluta (non è accolta

alcuna richiesta di accesso verso porzioni di registro "proibite") può cedere il passo a una azione di mascheratura più morbida, in cui sono ammesse richieste di accesso, con una configurazione di mascheratura (per es., una inversione logica di bit selezionati) applicata ai dati restituiti in risposta a tali richieste.

Fermi restando i principi di fondo, i dettagli e le forme di attuazione possono variare, anche in modo apprezzabile, rispetto a quanto è stato descritto, puramente a titolo di esempio, senza uscire dall'ambito di protezione.

L'ambito di protezione è determinato dalle rivendicazioni annesse.

RIVENDICAZIONI

1. Dispositivo a semiconduttore (1), comprendente:

almeno una porzione di registro (14) configurata per avere segnali digitali memorizzati in essa, in cui il dispositivo a semiconduttore (1) è configurato (IF; 110, 112; 10A a 10E) per la comunicazione con almeno un ulteriore dispositivo (16), in cui l'almeno una porzione di registro (14) è esposta a richieste di accesso per accedere all'almeno una porzione di registro (14) durante la comunicazione del dispositivo a semiconduttore (1) con l'almeno un ulteriore dispositivo (16), e

una circuiteria di schermo di registro (100) accoppiata all'almeno una porzione di registro (14), la circuiteria di schermo di registro (100) comprendendo una circuiteria di rilevazione di accesso (200) configurata per rilevare le richieste di accesso per accedere all'almeno una porzione di registro (14) durante la comunicazione del dispositivo a semiconduttore (1) con l'almeno un ulteriore dispositivo (16),

in cui la circuiteria di schermo di registro (100) è configurata per essere attivata selettivamente (208) in una modalità di schermo di registro per schermare l'almeno una porzione di registro (14) da dette richieste di accesso, in cui la circuiteria di schermo di registro (100), quando attivata in detta modalità di schermo di registro, impedisce l'accesso a detta almeno una porzione di registro (14) in risposta alle richieste di accedere all'almeno una porzione di registro (14) rilevate dalla circuiteria di rilevazione di accesso (200).

2. Dispositivo a semiconduttore (1) secondo la rivendicazione 1, comprendente celle programmabili una volta sola, OTP (102, 104) configurate per controllare l'attivazione della circuiteria di schermo di registro (100).

3. Dispositivo a semiconduttore (1) secondo la rivendicazione 2, in cui le celle programmabili una volta sola, OTP (102, 104) sono implementate come fusibili elettronici.

4. Dispositivo a semiconduttore (1) secondo una qualsiasi delle rivendicazioni da 1 a 3, in cui il dispositivo a semiconduttore (1) è configurato per la comunicazione con almeno un ulteriore dispositivo (16) tramite una circuiteria di interconnessione (110) e in cui la circuiteria di schermo di registro (100) è inclusa nella circuiteria di interconnessione (110).

5. Dispositivo a semiconduttore (1) secondo la rivendicazione 4, in cui la circuiteria di interconnessione (110) ha associato un bridge di protocollo (112) e in cui il dispositivo (1) comprende una circuiteria di schermo di registro (100) inclusa in detto bridge di protocollo (112).

6. Dispositivo a semiconduttore (1) secondo la rivendicazione 4 o la rivendicazione 5, in cui la circuiteria di schermo di registro (100) è inclusa in un decodificatore o un bridge di interconnessione in detta circuiteria di interconnesione (110).

7. Dispositivo a semiconduttore (1) secondo una qualsiasi delle rivendicazioni precedenti, in cui la circuiteria di schermo di registro (100) è configurata per essere attivata selettivamente (208) in una modalità di mascheratura di registro in cui, quando attivata in detta modalità di mascheratura di registro, la circuiteria di schermo di registro (100) consente l'accesso a detta almeno una porzione di registro (14) in risposta alle richieste di accesso all'almeno una porzione di registro (14) rilevate dalla circuiteria di rilevazione di accesso (200) e applica una configurazione di mascheratura di bit (214) ai dati (DB) restituiti in risposta a dette richieste di accesso dall'almeno una porzione di registro (14).

8. Dispositivo a semiconduttore (1) secondo la rivendicazione 7, in cui detta configurazione di mascheratura di bit (214) comprende una inversione logica di bit selezionati (OTP bus) nei bit dati (DB) restituiti dall'almeno una porzione di registro (14) in risposta a dette richieste di accesso all'almeno una porzione di registro (14).

9. Procedimento di funzionamento di un dispositivo a semiconduttore (1) secondo una qualsiasi delle rivendicazioni precedenti, il procedimento comprendendo:

identificare nel dispositivo a semiconduttore (1) almeno una porzione di registro (14) configurata per avere memorizzati in essa segnali digitali previsti per essere esclusi dalla comunicazione con l'almeno un ulteriore dispositivo (16), e

attivare (102) in detta modalità di schermo di registro la circuiteria di schermo di registro (100)

accoppiata con l'almeno una porzione di registro (14) identificata in cui, quando attivata in detta modalità di schermo di registro, la circuiteria di schermo di registro (100) scherma da dette richieste di accesso l'almeno una porzione di registro (14) identificata impedendo l'accesso a detta almeno una porzione di registro (14) identificata in risposta alle richieste di accesso all'almeno una porzione di registro (14) rilevate dalla circuiteria di rilevazione di accesso (200).

10. Procedimento secondo la rivendicazione 9, applicato al funzionamento di un dispositivo a semiconduttore (1) secondo la rivendicazione 7 o la rivendicazione 8, il procedimento comprendendo:

identificare nel dispositivo a semiconduttore (1) almeno un'ulteriore porzione di registro (14) configurata per avere memorizzati in essa segnali digitali previsti per avere applicata una configurazione di mascheratura di bit (214) nella comunicazione con l'almeno un ulteriore dispositivo (16), e

attivare (102) la circuiteria di schermo di registro (100) in detta modalità di mascheratura di registro in cui, quando attivata in detta modalità di mascheratura di registro, la circuiteria di schermo di registro (100) consente l'accesso a detta almeno un'ulteriore porzione di registro (14) identificata ed applica una configurazione di mascheratura di bit (214) ai dati (DB) restituiti in risposta a dette richieste di accesso da detta almeno un'ulteriore porzione di registro (14) identificata.

FIG. 1

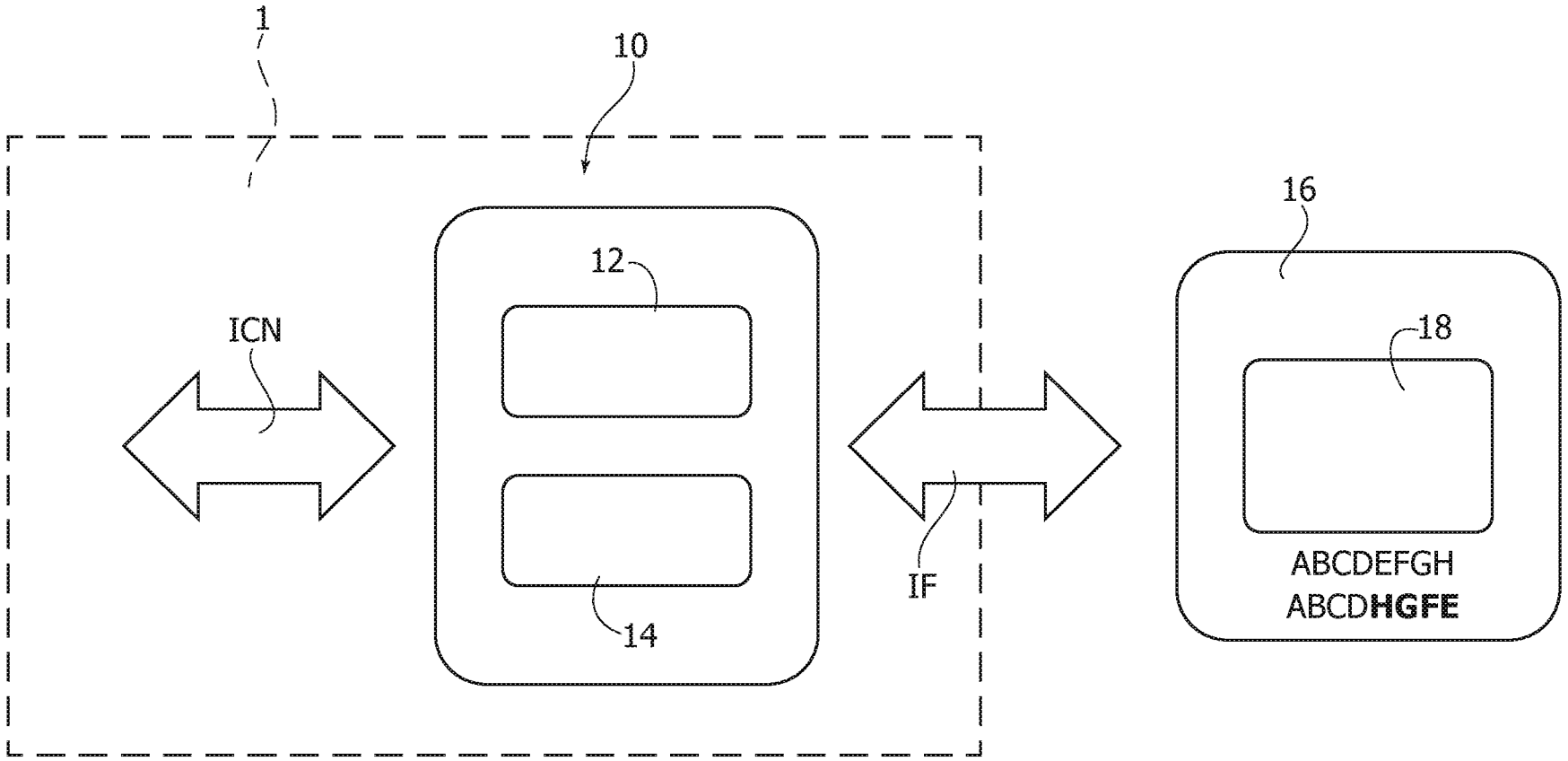


FIG. 2

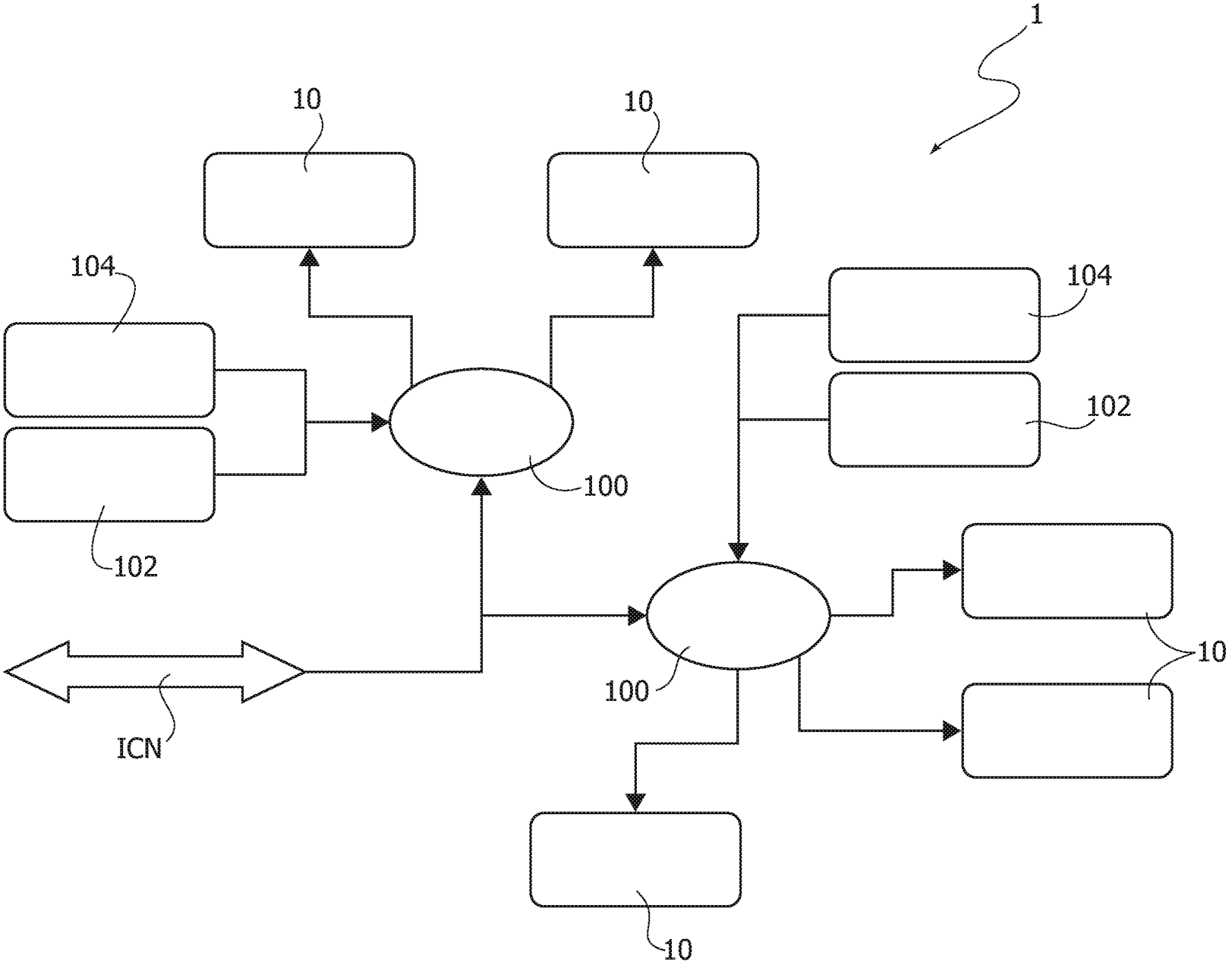


FIG. 3

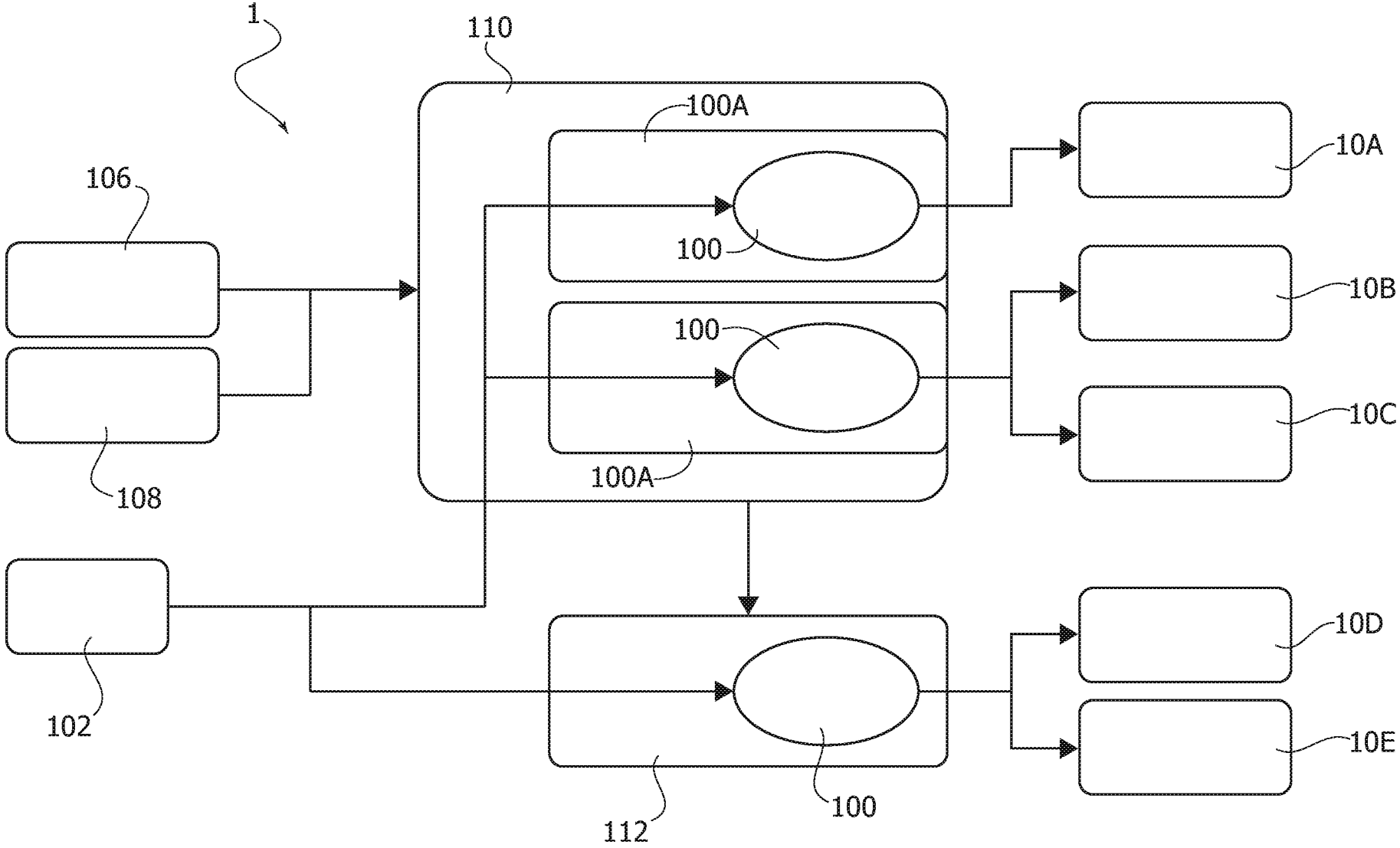


FIG. 4

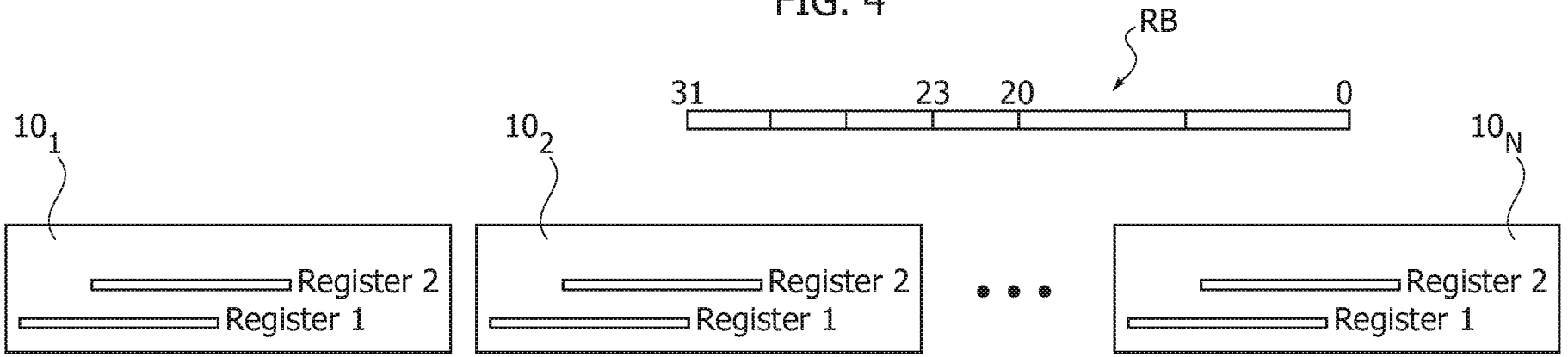


FIG. 5

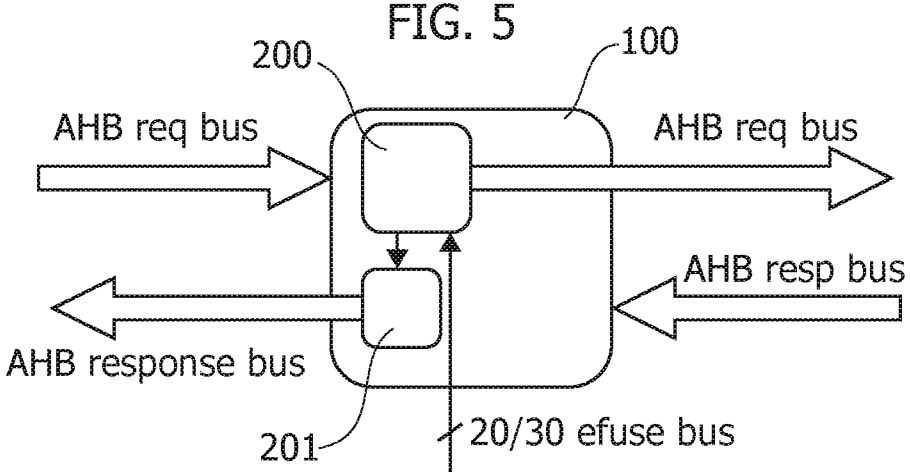


FIG. 6

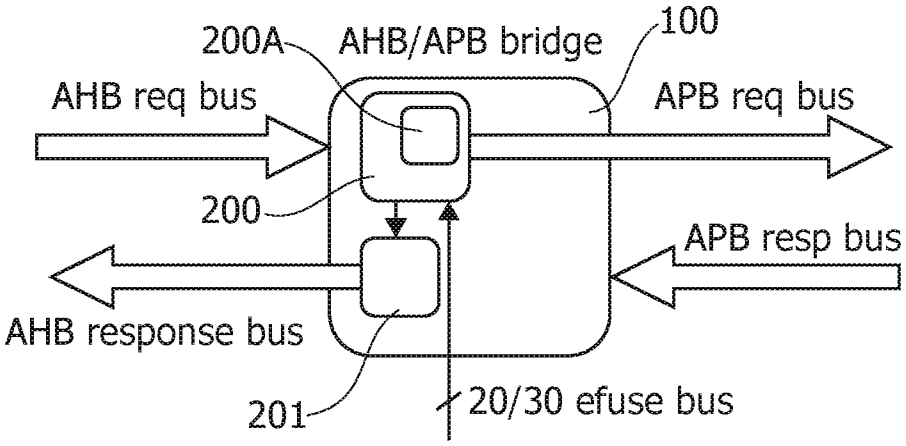


FIG. 7

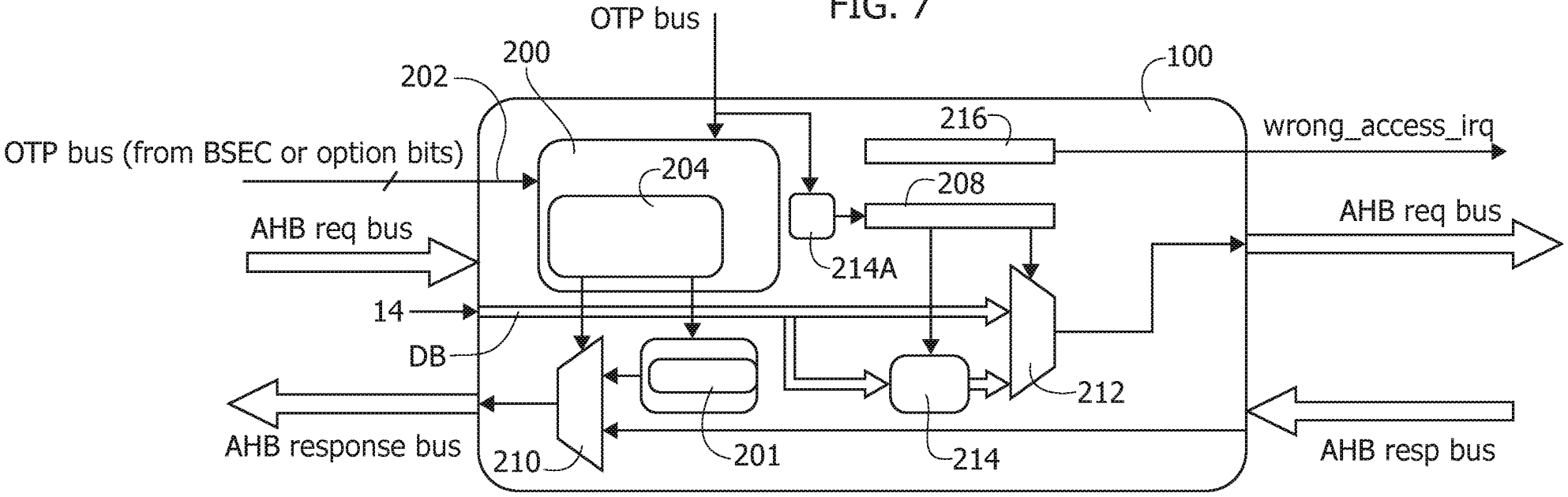
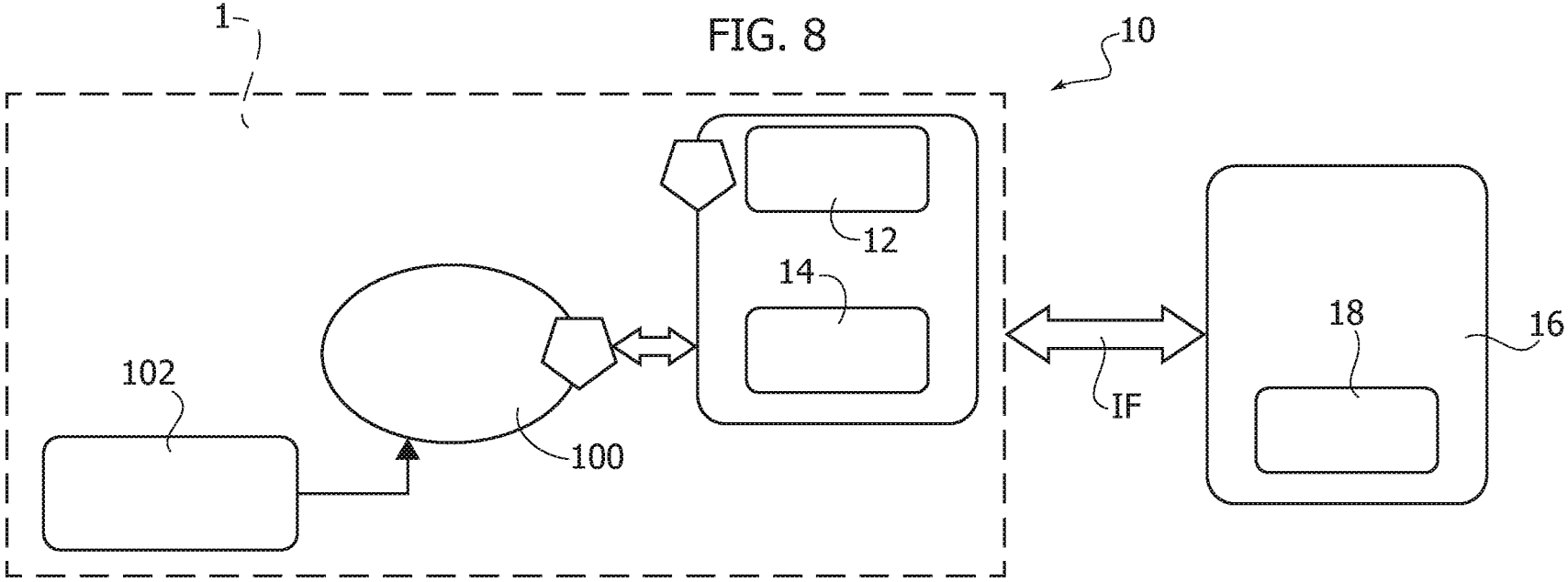

OTP bus
200
202
100
216
wrong_access_irq
OTP bus (from BSEC or option bits)
204
208
AHB req bus
AHB req bus
214A
14
DB
212
AHB response bus
210
201
214
AHB resp bus

FIG. 8


1
10
12
14
18
16
102
100
IF