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

UIBM

DOMANDA DI INVENZIONE NUMERO	102021000030332
Data Deposito	30/11/2021
Data Pubblicazione	30/05/2023

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	44

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	55

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	76

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	79

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	85

Titolo

Sistema di elaborazione, relativo circuito integrato, dispositivo e procedimento

ESCRIZIONE dell'invenzione industriale dal titolo:
"Sistema di elaborazione, relativo circuito integrato, dispositivo e procedimento"
di: STMicroelectronics Application GmbH, di nazionalità tedesca, Bahnhofstrasse 18, 85609 Aschheim, Germania; STMicroelectronics International N.V., di nazionalità svizzera, Chemin du Champ-des-Filles 39, 1228 Plan-les-Ouates, Geneva, Svizzera; STMicroelectronics S.r.l., di nazionalità italiana, Via C. Olivetti, 2 - 20864 Agrate Brianza (Provincia di Monza e Brianza), Italia
Inventori designati: Asif Rashid ZARGAR, Nicolas Bernard GROSSIER, Charul JAIN, Roberto COLOMBO.
Depositata il: 30 novembre 2021

* * *

TESTO DELLA DESCRIZIONE

Campo Tecnico

Le forme di attuazione della presente descrizione sono relative alla protezione dei sistemi di elaborazione dalle modifiche dei registri.

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), 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 periferiche/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 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.

Le future generazioni di sistemi di elaborazione, in particolare i microcontrollori dedicati alle applicazioni automotive, presenteranno un aumento apprezzabile della complessità, dovuto principalmente al numero crescente di funzionalità (come nuovi protocolli, nuove caratteristiche, ecc.) e ai vincoli stringenti concernenti le condizioni di funzionamento del sistema (come un consumo di potenza più basso, maggiore velocità e potenza di calcolo, ecc.).

In parallelo, anche il framework di sicurezza di ciascun sistema di elaborazione 10 diventa sempre più complesso. Di solito, il framework di sicurezza è basato sul concetto di

protezione delle risorse, cioè, dato un insieme di risorse, il framework è progettato in modo tale che l'accesso a una o più risorse possa essere bloccato o concesso selettivamente in base a specifiche condizioni. Per esempio, spesso l'accesso a date risorse, come aree di memoria della memoria non volatile 104 e/o un'interfaccia di debug, può essere bloccato memorizzando uno o più bit in locazioni di memoria riservate di una memoria non volatile 104. In aggiunta o in alternativa, spesso l'accesso alla risorsa può essere bloccato finché non è fornita la data password, per es., mediante il microprocessore 102 o un'interfaccia di comunicazione IF.

A questo riguardo, lo stato per quanto riguarda se l'accesso a una data risorsa è bloccato o concesso è memorizzato di solito in un registro, per es., implementato con uno o più flip-flop. Tuttavia, questo comporta che un hacker potrebbe tentare di modificare il contenuto di tali registri al fine di concedere l'accesso a una risorsa bloccata.

Sintesi

In considerazione di quanto precede, uno scopo delle varie forme di attuazione della presente descrizione è di fornire soluzioni atte a proteggere i registri, in particolare i registri di configurazione usati per memorizzare informazioni di sicurezza, come i registri di configurazione configurati per memorizzare dati che identificano se l'accesso a una risorsa è concesso o bloccato e/o registri di configurazione configurati per memorizzare una o più password di riferimento.

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 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. Specificamente, il sistema di elaborazione comprende una pluralità di elementi di memorizzazione, in cui ciascun elemento di memorizzazione comprende un latch o un flip-flop ed è configurato per ricevere una richiesta di scrittura comprendente un bit di dati e per memorizzare il bit di dati ricevuto nel latch o nel flip-flop. Di conseguenza, un circuito hardware può essere configurato per cambiare operazione in funzione del livello logico memorizzato nel latch o nel flip-flop di almeno un primo elemento di memorizzazione della pluralità di elementi di memorizzazione.

Specificamente, in varie forme di attuazione, i primi elementi di memorizzazione possono essere usati per memorizzare dati di configurazione relativi alla sicurezza. Per esempio, come sarà descritto in maggiore dettaglio in seguito, il circuito hardware può comprendere almeno un sotto-circuito, come una risorsa/periferica, un controllore di memoria o un microprocessore, e un circuito di protezione configurato per ricevere un comando di controllo per il sotto-circuito ed eseguire selettivamente il (o inibire selettivamente l'esecuzione del) comando di controllo, cioè, inoltrare (o non inoltrare) selettivamente il comando di controllo al sotto-circuito. Per esempio, in varie forme di attuazione, il sistema di elaborazione comprende un microprocessore e/o un'interfaccia di debug configurati per

fornire un tale comando di controllo per controllare il funzionamento del circuito hardware. Per esempio, il comando di controllo può essere una richiesta di lettura o di scrittura.

Di conseguenza, il circuito di protezione può eseguire selettivamente il comando di controllo (almeno) in funzione del livello logico memorizzato nel latch o nel flip-flop di un primo elemento di memorizzazione. Per esempio, il bit di dati memorizzato nel primo elemento di memorizzazione può corrispondere a dati di configurazione e/o a dati di ciclo di vita ("life-cycle").

Di conseguenza, in varie forme di attuazione, il sistema di elaborazione comprende anche una memoria non volatile configurata per memorizzare bit di dati per la pluralità di elementi di memorizzazione, e un circuito di configurazione hardware configurato per leggere i bit di dati dalla memoria non volatile e generare richieste di scrittura al fine di memorizzare i bit di dati negli elementi di memorizzazione.

In varie forme di attuazione, il sistema di elaborazione è configurato per proteggere i dati memorizzati nel latch o nel flip-flop del primo elemento (dei primi elementi) di memorizzazione da attacchi di manomissione. A questo scopo, il primo elemento di memorizzazione comprende un ulteriore latch o flip-flop ed è configurato per memorizzare, in risposta alla richiesta di scrittura, la versione invertita del bit di dati ricevuto nell'ulteriore latch o flip-flop. Inoltre, il primo elemento di memorizzazione comprende anche un circuito logico combinatorio configurato per confrontare il livello logico memorizzato nel latch o nel flip-flop del primo elemento di memorizzazione con il livello logico memorizzato nell'ulteriore latch o flip-flop del primo elemento di memorizzazione. Specificamente, in varie forme

di attuazione, il primo elemento di memorizzazione è configurato per deasserire un primo segnale di manomissione associato al primo elemento di memorizzazione quando i livelli logici sono differenti, e per asserire il primo segnale di manomissione quando i livelli logici sono gli stessi.

Di conseguenza, in varie forme di attuazione, il circuito hardware è configurato per cambiare operazione anche in funzione del primo segnale di manomissione. Per esempio, un circuito di protezione del circuito hardware può essere configurato per eseguire selettivamente il comando di controllo in funzione del livello logico memorizzato nel latch o nel flip-flop del primo elemento di memorizzazione e del primo segnale di manomissione. Per esempio, il circuito di protezione può essere configurato per eseguire (cioè, inoltrare) il comando di controllo quando il latch o il flip-flop del primo elemento di memorizzazione ha memorizzato un primo livello logico e il primo segnale di manomissione è deasserito, e per inibire l'esecuzione del (cioè, non inoltrare il) comando di controllo quando il latch o il flip-flop del primo elemento di memorizzazione ha memorizzato un secondo livello logico o il primo segnale di manomissione è asserito.

In alternativa, il circuito di protezione può essere configurato per eseguire selettivamente il comando di controllo in funzione di un segnale di controllo, e il circuito hardware o il primo elemento di memorizzazione può comprendere un circuito logico combinatorio configurato per determinare se il primo segnale di manomissione è asserito. In questo caso, in risposta alla determinazione che il primo segnale di manomissione è deasserito, il circuito logico combinatorio può impostare il primo segnale di controllo al

valore logico memorizzato nel latch o nel flip-flop del primo elemento di memorizzazione. Per contro, in risposta alla determinazione che il primo segnale di manomissione è asserito, il circuito logico combinatorio può impostare il primo segnale di controllo a un valore di manomissione predeterminato.

Generalmente, il circuito di protezione può anche essere configurato per gestire l'accesso a una pluralità di sotto-circuiti e/o di aree di memoria, in cui a ciascun sotto-circuito e/o a ciascuna area di memoria è associato almeno un rispettivo primo elemento di memorizzazione. In questo caso, il circuito di protezione può essere configurato per inibire l'esecuzione del comando di controllo (a un sottoinsieme o a tutti i sotto-circuiti e/o tutte le aree di memoria) quando almeno uno dei primi segnali di manomissione forniti dalla pluralità di primi elementi di memorizzazione è asserito.

In varie forme di attuazione, il circuito hardware può anche comprendere un circuito di verifica di password configurato per ricevere un comando di verifica di password dal microprocessore e/o dall'interfaccia di debug, in cui il comando di verifica di password comprende una password. In seguito, il circuito di verifica di password può confrontare la password con una chiave di riferimento, in cui la chiave di riferimento è determinata in funzione dei livelli logici memorizzati nel latch o nel flip-flop di una pluralità di secondi elementi di memorizzazione della pluralità di elementi di memorizzazione, e può asserire un segnale di sovrascrittura quando la password corrisponde alla chiave di riferimento. Di conseguenza, in questo caso, il circuito di protezione può essere configurato per eseguire (cioè,

inoltrare) il comando di controllo quando il segnale di sovrascrittura è asserito.

Per esempio, in varie forme di attuazione, anche ciascuno dei secondi elementi di memorizzazione comprende un ulteriore latch o flip-flop e un circuito logico combinatorio configurato per asserire selettivamente un secondo segnale di manomissione confrontando il livello logico memorizzato nel latch o nel flip-flop del rispettivo secondo elemento di memorizzazione con il livello logico memorizzato nell'ulteriore latch o flip-flop del rispettivo secondo elemento di memorizzazione.

In varie forme di attuazione, anche il circuito di verifica di password può considerare i rispettivi segnali di manomissione. Per esempio, il circuito di verifica può essere configurato per asserire il segnale di sovrascrittura quando la password corrisponde alla chiave di riferimento e i secondi segnali di manomissione forniti dai secondi elementi di memorizzazione sono deasseriti, e per deasserire il segnale di sovrascrittura quando la password non corrisponde alla chiave di riferimento o almeno uno dei secondi segnali di manomissione forniti dai secondi elementi di memorizzazione è asserito.

In aggiunta o in alternativa, il circuito di protezione può essere configurato per inibire l'esecuzione del comando di controllo quando almeno uno dei secondi segnali di manomissione forniti dai secondi elementi di memorizzazione è asserito.

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 tipico sistema elettronico comprendente una pluralità di sistemi di elaborazione;

- la Figura 2 rappresenta un esempio di un sistema di elaborazione;

- la Figura 3 rappresenta una forma di attuazione di un sistema di elaborazione;

- la Figura 4 rappresenta una forma di attuazione dell'architettura di sicurezza di un sistema di elaborazione;

- la Figura 5 rappresenta una forma di attuazione dell'architettura di sicurezza di un sistema di elaborazione comprendente un circuito di verifica di password;

- la Figura 6 rappresenta una forma di attuazione dell'architettura di sicurezza di un sistema di elaborazione comprendente un circuito di verifica di password e un repository di password temporaneo;

- le Figure 7 e 8 rappresentano forme di attuazione di un sistema di elaborazione comprendente un circuito di configurazione e client di dati di configurazione; e

- le Figure da 9 a 12 rappresentano forme di attuazione di elementi di memorizzazione per i client di dati di configurazione delle Figure 7 e 8.

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 3 a 12 che seguono, le parti, gli elementi o i componenti che sono già stati descritti con riferimento alle Figure 1 e 2 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.

La Figura 3 rappresenta una forma di attuazione di un sistema di elaborazione 10a secondo la presente descrizione.

Specificamente, nella forma di attuazione considerata, il sistema di elaborazione 10a comprende almeno un core di elaborazione 102 integrato in un circuito integrato 30, come n core di elaborazione 102_1...102_n, in cui l'uno o più core di elaborazione 102 sono connessi a un sistema di comunicazione (on-chip) 114. 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 sull'architettura di bus 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. Nella forma di attuazione considerata, l'interfaccia 1022 è un'interfaccia master configurata per inoltrare una 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. In varie forme di attuazione, il core di elaborazione 102a può anche comprendere 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 di comunicazione 1022 del primo microprocessore, il sistema di comunicazione 114 e l'interfaccia di comunicazione 1024 del secondo microprocessore). Per esempio, a questo scopo il sistema di comunicazione 114 può comprendere in aggiunta a un bus di sistema o un NoC, anche un bus di coprocessore aggiuntivo, per es., che connette i microprocessori 1020 dello stesso core di elaborazione 102a o di tutti i core di elaborazione 102a.

In varie forme di attuazione, 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 varie forme di attuazione, queste memorie sono memorie di sistema, cioè, condivise per i core di elaborazione 102_1...102_n. Per esempio, in varie forme di attuazione, il sistema di elaborazione 10a comprende 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 in un circuito integrato 30 comprendente il (i) core di elaborazione 102 o possono essere connesse all'esterno del circuito integrato 30.

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. 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. Per esempio, ciascuna delle risorse 106 può essere connessa al sistema di comunicazione 114 mediante un'interfaccia slave 1062 della risorsa 106 e/o mediante un controllore DMA 107 comprendente un'interfaccia master configurata per scambiare dati direttamente inviando richieste di lettura o di scrittura al sistema di comunicazione 114.

Come rappresentato nella Figura 3, il circuito integrato 30 del sistema di elaborazione 10a può anche comprendere un'interfaccia di debug 50. Per esempio, una

tipica interfaccia di debug 50 comprende due sotto-circuiti: un'interfaccia di comunicazione 502, come un'interfaccia JTAG (Joint Test Action Group), CAN, SPI o un'interfaccia di comunicazione I^2C che gestisce lo scambio di dati con il dispositivo di debugging ("debugger") 52 esterno, e un circuito di debug 500 interno configurato per gestire le operazioni di debug, per es., inviando richieste di lettura o di scrittura mediante il sistema di comunicazione 114 o un bus di debug dedicato. In generale, il circuito di debug 500 può anche essere implementato mediante istruzioni software eseguite mediante un core di elaborazione 102, per es., ricevendo i comandi di debug mediante una delle interfacce di comunicazione IF del sistema di elaborazione 10a.

Come menzionato in precedenza, in varie forme di attuazione, il sistema di elaborazione 10a comprende un'architettura di sicurezza configurata per limitare l'accesso a una o più delle risorse del sistema di elaborazione 10a.

La Figura 4 rappresenta una forma di attuazione dell'architettura di sicurezza di un sistema di elaborazione 10a.

Come menzionato in precedenza, l'architettura di sicurezza di un sistema di elaborazione 10a, come un microcontrollore, ha come obiettivo di limitare l'accesso a uno o più dei circuiti del sistema di elaborazione 10a, indicati in seguito come risorse 110, come le memorie 104 e/o 104b, una o più delle unità di elaborazione 102 e/o una o più risorse 106.

Per esempio, come rappresentato nella Figura 4, una o più delle risorse 110 del sistema di elaborazione possono avere associato (per es., possono comprendere) un circuito di protezione 150 configurato per controllare l'accesso alla

rispettiva risorsa 110. Per esempio, rispettive richieste di accesso CMD possono essere ricevute da un'altra risorsa del sistema di elaborazione 10a, come l'unità di elaborazione 102 e/o l'interfaccia di debug 50.

Per esempio, in varie forme di attuazione, i circuiti di protezione 150 possono controllare l'accesso a una risorsa 110 target inoltrando selettivamente una lettura o una scrittura dalla risorsa sorgente (per es., un'unità di elaborazione 102 e/o l'interfaccia di debug 50) alla risorsa 110 target. Generalmente, questa lettura e/o scrittura può essere inoltrata mediante il sistema di comunicazione 114 (per es., nel caso di un core di elaborazione 102) o mediante un bus/sistema di comunicazione di debug dedicato (per es., nel caso di un'interfaccia di debug 50 hardware). Per esempio, i circuiti di protezione 150 possono essere configurati per:

- inoltrare selettivamente la lettura o scrittura dalla risorsa sorgente al sistema di comunicazione; e/o
- inoltrare selettivamente la lettura scrittura dal sistema di comunicazione alla risorsa 110 target.

Tuttavia, in generale, il circuito di protezione 150 può anche essere implementato all'interno delle risorse target e/o sorgente. Per esempio, come menzionato in precedenza, una tipica interfaccia di debug 50 comprende un'interfaccia di comunicazione 502 che gestisce lo scambio di dati con il debugger 52 esterno, e un circuito di debug 500 interno configurato per gestire le operazioni di debug. Di conseguenza, in questo caso, il circuito di protezione 150 può essere configurato per disattivare l'interfaccia di debug 50 interrompendo la connessione tra l'interfaccia di comunicazione 500 e il circuito di debug 502 interno e/o la

connessione dell'interfaccia di comunicazione 500 ai pin a cui può essere connesso un debugger 52 esterno.

Generalmente, mentre alcune risorse 110 possono non avere eventualmente affatto alcuna limitazione di accesso, l'accesso ad altre risorse 110 può essere bloccato (cioè, la protezione può essere attivata) di default o selettivamente in funzione di dati di configurazione. Per esempio, in varie forme di attuazione e come anche descritto in dettaglio nelle Pubblicazioni di Domanda di Brevetto Statunitense US 2018/0357015 A1 e US 2018/0357012 A1, che sono incorporate qui tramite citazione a questo scopo, le protezioni di una data risorsa possono essere attivate selettivamente in funzione dello stadio del ciclo di vita del sistema di elaborazione 10a come indicato dai dati del ciclo di vita LCD e/o dai dati di configurazione CD. Per esempio, ciascuna protezione 150 del sistema di elaborazione 10a può essere in uno dei seguenti stati:

a) i dati del ciclo di vita LCD indicano che la protezione è disabilitata indipendentemente dai dati di configurazione CD;

b) i dati del ciclo di vita LCD indicano che la protezione può essere abilitata selettivamente e i dati di configurazione CD indicano che la protezione è disabilitata;

c) i dati del ciclo di vita LCD indicano che la protezione può essere abilitata selettivamente e i dati di configurazione indicano che la protezione è abilitata; o

d) i dati del ciclo di vita LCD indicano che la protezione è abilitata indipendentemente dai dati di configurazione CD.

Per esempio, nel contesto di una memoria 104 e/o 104b, l'intervallo di memoria della memoria può essere diviso in settori, e a ciascun settore possono essere associati uno o

più bit di rispettivi dati di configurazione CD, che così indicano se un accesso in lettura e/o uno in scrittura al rispettivo settore di memoria è permesso oppure no.

La Figura 5 rappresenta una forma di attuazione di un'architettura di sicurezza modificata del sistema di elaborazione 10a.

Specificamente, nella forma di attuazione considerata, al fine di concedere l'accesso a risorse protette, il sistema di elaborazione 10a comprende un circuito per sovrascrivere una o più delle protezioni quando è fornita una specifica password. Generalmente, alcune protezioni 150, una volta attivate, possono anche non essere più disattivate, o una data password può soltanto disattivare un dato sottoinsieme di protezioni. Per esempio, non si può mai accedere alle aree di memoria protette in lettura che contengono dati relativi alla sicurezza, come le chiavi crittografiche, perfino quando è fornita una password.

Nell'esempio considerato, almeno una password/parola chiave ("keyword") di riferimento RK è memorizzata in qualche modo nel sistema di elaborazione 10a. Per esempio, la password di riferimento RK può essere cablata in hardware ("hardwired") o memorizzata in una memoria non volatile 104 del sistema di elaborazione 10a, come la memoria di programma non volatile 104a. In quest'ultimo caso, è richiesto preferibilmente che il sistema di elaborazione 10a limiti l'accesso in lettura all'area di memoria contenente la password di riferimento RK al fine di assicurare che la password di riferimento RK sia tenuta segreta. Per esempio, possibili soluzioni per memorizzare una parola chiave di riferimento in una memoria non volatile sono descritte nelle domande di brevetto citate in precedenza.

Nell'esempio considerato, il sistema di elaborazione 10a comprende inoltre un circuito di verifica di password 152.

Di conseguenza, al fine di disattivare almeno una protezione, l'utente dovrebbe potere fornire un comando di verifica di password VPW comprendente una password/parola chiave K al circuito di verifica di password 152. Per esempio, nella forma di attuazione considerata, l'utente può fornire la password K al circuito di verifica di password 152 mediante istruzioni software eseguite dall'unità di elaborazione 102 del sistema di elaborazione 10a e/o mediante un'interfaccia di comunicazione del sistema di elaborazione 10a, come mediante un'interfaccia CAN o un'interfaccia di debug 50 (per es., JTAG) connessa a un debugger 52 esterno.

Per esempio, in varie forme di attuazione, i blocchi 110, il circuito di verifica di password 152 e l'interfaccia IF e/o l'unità di elaborazione 102 possono essere connessi attraverso un sistema di comunicazione adeguato, come il sistema di comunicazione 114. In questo caso, il comando CMD e il comando di verifica di password VPW possono essere trasmessi sopra lo stesso bus, specificando come indirizzo target l'indirizzo di un blocco 110 (per un comando CMD) o del circuito di verifica di password 152 (per un comando di verifica di password VPW).

Di conseguenza, una volta che il circuito di verifica di password 152 ha ricevuto il comando di verifica di password VPW comprendente la password K, il circuito di verifica di password 152 può ottenere la password di riferimento RK e confrontare la password K con la password di riferimento RK e, nel caso in cui le due password concordino ("match"), il circuito di verifica di password 152 può generare un segnale di sovrascrittura OW, che è

inviato a uno o più circuiti di protezione 150. Di conseguenza, in risposta al segnale di sovrascrittura OW, il circuito (i circuiti) di protezione 150 può (possono) disattivare almeno una parte della rispettiva protezione.

La Figura 6 rappresenta una forma di attuazione dell'architettura di sicurezza di un sistema di elaborazione 10a in linea con la descrizione della Pubblicazione della Domanda di Brevetto Statunitense US 2019/026498 A1, che è incorporata qui tramite citazione.

Specificamente, in confronto alla Figura 5, il sistema di elaborazione 10a comprende inoltre un circuito di caricamento di password 154 e un repository di password temporaneo 156.

Di conseguenza, nell'esempio considerato, il circuito di verifica di password 152 non accede dinamicamente alla (alle) password di riferimento RK originale (originali), che è cablata (sono cablate) in hardware o è memorizzata (sono memorizzate) preferibilmente nella memoria non volatile 104. Per contro, il circuito di caricamento di password 154 legge la (le) password di riferimento RK una volta e memorizza la (le) password di riferimento RK nel repository di password temporaneo 156, che è implementato, per es., con registri, che possono essere letti soltanto dal circuito di verifica di password 152. Di conseguenza, il circuito di verifica di password 152 può confrontare la password K ricevuta con una password di riferimento RK memorizzata nel repository di password temporaneo 156, in cui il percorso di lettura tra il circuito di verifica di password 152 e il repository di password temporaneo 156 non è condiviso con altre risorse del sistema di elaborazione 10a e di conseguenza non può essere spiato.

Di conseguenza, come descritto in precedenza, in varie forme di attuazione, le protezioni possono essere attivate e similmente anche i blocchi 110 possono essere configurati in base ai dati del ciclo di vita LCD e/o ai dati di configurazione CD.

Per esempio, la Figura 7 rappresenta un esempio di un sistema di elaborazione 10a, in cui i dati di configurazione CD possono essere scritti in specifiche aree di una memoria non volatile e possono essere recuperati quando il sistema di elaborazione 10a è alimentato.

Per esempio, i dati di configurazione CD possono essere memorizzati nella memoria non volatile 104 e/o in una memoria non volatile aggiuntiva, come una memoria programmabile una volta sola (OTP, "One-Time Programmable"), per es., implementata con fusibili. Per esempio, può essere usata la memoria 104, nel caso in cui la memoria sia integrata con il microprocessore 102 nello stesso circuito integrato 30. Per contro, può essere usata una memoria non volatile aggiuntiva nel caso in cui la memoria 104 sia una memoria esterna. Di conseguenza, in varie forme di attuazione, i dati di configurazione CD sono memorizzati in una memoria non volatile del circuito integrato 30.

Per esempio, tali dati di configurazione CD possono includere dati di calibrazione usati per garantire che il comportamento dell'hardware sia uniforme, compensando con ciò possibili tolleranze di processo di produzione. Per esempio, questo si applica spesso alla calibrazione dei componenti analogici del sistema di elaborazione, come un sensore di temperatura, un convertitore analogico/digitale, un riferimento di tensione, ecc. Inoltre, come menzionato in precedenza, i dati di configurazione CD possono anche essere usati per personalizzare (customizzare) il comportamento

dell'hardware, per es., dei blocchi hardware 110 e/o dei circuiti di protezione 150, secondo necessità di applicazione differenti. Per esempio, come menzionato in precedenza, una volta che il firmware del sistema di elaborazione 10a è stato memorizzato nel sistema di elaborazione 10a, alcuni dati di configurazione CD possono essere scritti al fine di disattivare l'interfaccia di debug 50, che potrebbe essere usata, per es., per scaricare il firmware del sistema di elaborazione 10a. Così, generalmente una prima parte dei dati di configurazione CD può essere scritta dal produttore dell'hardware del sistema di elaborazione (per es., il produttore di un circuito integrato) e/o una seconda parte dei dati di configurazione CD può essere scritta dallo sviluppatore del firmware del sistema di elaborazione 10a.

In varie forme di attuazione, i dati di configurazione programmati CD sono letti durante una fase di configurazione, che di solito inizia non appena il sistema di elaborazione 10a è alimentato.

Specificamente, come rappresentato nella Figura 7, il sistema di elaborazione 10a può comprendere a questo scopo un circuito di configurazione 108 configurato per leggere i dati di configurazione CD dalla memoria non volatile 104, e per distribuire questi dati di configurazione CD all'interno del sistema di elaborazione 10a. Per esempio, nella forma di attuazione considerata, i dati di configurazione CD sono memorizzati in aree di memoria riservate, per es., sotto forma di una pluralità di locazioni di memoria consecutive. Di conseguenza, nella forma di attuazione considerata, il circuito di configurazione 108 accede alle aree di memoria riservate contenenti i dati di configurazione CD, legge i dati di configurazione CD e trasmette i dati di

configurazione CD a un rispettivo blocco 110 e/o circuito di protezione 150 all'interno del sistema di elaborazione 10a. Come menzionato in precedenza, il blocco 110 può corrispondere a un qualsiasi blocco del sistema di elaborazione 10a che richiede dati di configurazione e può corrispondere all'unità di elaborazione 102, a una risorsa hardware 106 o perfino a una memoria (per es., la memoria 104a).

Per esempio, al fine di distribuire i dati di configurazione CD, ciascun blocco 110 e ciascun circuito di protezione 150 possono avere associato un rispettivo client di dati di configurazione 112. Per esempio, nella Figura 7 sono rappresentati due client di dati di configurazione 112a, 112b che forniscono i dati di configurazione a un circuito 110 e ai circuiti di protezione 150, rispettivamente. Generalmente, ciascun client di dati di configurazione 112 può essere associato in modo univoco a un singolo circuito 110 o a un singolo circuito di protezione 150, e può fornire dati di configurazione soltanto al circuito 110 o al circuito di protezione 150 associato, per es., una specifica risorsa hardware 106. Tuttavia, il client di dati di configurazione 112 può anche essere associato a una pluralità di blocchi hardware 110 e/o di circuiti di protezione 150. Per esempio, in varie forme di attuazione, lo stesso client di dati di configurazione 112 è usato per fornire dati di configurazione CD a un circuito 110 e al circuito di protezione 150 associato a questo blocco hardware 110. In generale, i client di dati di configurazione possono anche essere integrati nel rispettivo circuito 110 o circuito di protezione 150.

Di conseguenza, nella forma di attuazione considerata, il circuito di configurazione 108 può determinare per ciascun blocco target 110/150 da configurare, i rispettivi dati di

configurazione (selezionati tra i dati di configurazione CD) e può trasmettere i dati di configurazione associati al blocco target 110/150 al client di dati di configurazione 112 associato al blocco target 110/150. Similmente, mentre legge i dati di configurazione CD dalla memoria 104, il circuito di configurazione 108 può determinare il blocco (i blocchi) target per le informazioni di configurazione correnti e può inviare i dati di configurazione correnti al (ai) client di dati di configurazione associato (associati) al rispettivo blocco (ai rispettivi blocchi) target. Generalmente, può essere usata una comunicazione qualsiasi per trasmettere i dati di configurazione CD ai client di dati di configurazione 112, comprendendo comunicazioni sia seriali sia parallele. Per esempio, il circuito di configurazione 108 e i client di dati di configurazione 112 possono essere connessi mediante un bus 109, corrispondente anche eventualmente al sistema di comunicazione 114, e ciascun client di dati di configurazione 112 può avere associato un rispettivo indirizzo target.

Di conseguenza, ciascun client di dati di configurazione 112 è configurato per ricevere i dati di configurazione dal modulo 108, memorizzarli nel registro interno, per es., memorizzarli in uno o più latch o flip-flop interni. I dati memorizzati nel registro possono quindi essere usati per generare uno o più segnali, che influenzano il comportamento di uno o più blocchi hardware 110 e/o circuiti di protezione 150.

In varie forme di attuazione, il meccanismo descritto in precedenza è usato anche per trasmettere le password di riferimento RK al repository di password temporaneo 156. Specificamente, in varie forme di attuazione, la (le) password di riferimento RK è memorizzata (sono memorizzate)

insieme ai dati di configurazione CD nella memoria 104, e uno o più client di dati di configurazione 112c sono associati (preferibilmente in modo univoco) al repository di password temporaneo 156. Di conseguenza, in varie forme di attuazione, il circuito di configurazione 108 legge anche la (le) password di riferimento RK insieme agli altri dati di configurazione CD dalla memoria 104 e invia la (le) password di riferimento RK al (ai) client di dati di configurazione 112c associato (associati) al repository di password temporaneo 156, caricando con ciò la (le) password di riferimento RK nel repository di password temporaneo 156.

La Figura 8 rappresenta a questo riguardo una possibile forma di attuazione della comunicazione tra il circuito di configurazione 108 e i client di dati di configurazione 112 in linea con la descrizione di US 2019/026498 A1.

Specificamente, anche in questo caso, il sistema di elaborazione 10a comprende un circuito di configurazione 108 configurato per leggere i dati di configurazione CD da una o più memorie non volatili 104 e una pluralità di client di dati di configurazione 112 configurati per ricevere rispettivi dati di configurazione CD dal circuito di configurazione 108 e per distribuirli tra i blocchi 110/150/156 che richiedono dati di configurazione. Per esempio, come menzionato in precedenza, ciascun client di dati di configurazione 112 può essere associato in modo univoco a un rispettivo circuito 110/150/156. Per esempio, nella forma di attuazione considerata, il sistema di elaborazione 10a comprende di nuovo tre gruppi di client di dati di configurazione 112a, 112b e 112c.

Nella forma di attuazione considerata, il circuito di configurazione 108 comprende un modulo di lettura di dati 1080 configurato per leggere i dati di configurazione CD

dalla memoria 104 e un modulo di smistamento 1082 configurato per trasmettere i dati di configurazione ai client di dati di configurazione 112.

Come menzionato in precedenza, può essere usata una comunicazione qualsiasi per la comunicazione tra il modulo di smistamento 1082 e i client di dati di configurazione 112. Per esempio, in varie forme di attuazione, la comunicazione tra il modulo di smistamento 1082 e i client di dati di configurazione 112 è basata su trame ("frame") di dati secondo un dato formato, detto in seguito Formato di Configurazione di Dispositivo (DCF, "Device Configuration Format"). Per esempio, in varie forme di attuazione, ciascun frame di dati comprende due campi: il carico utile ("payload") (cioè, i dati reali), detto *carico utile di Formato DCF*, e possibili attributi di dati aggiuntivi usati per identificare il ricevitore dei dati, detti *attributi di formato DCF*, in cui il ricevitore è uno dei client di dati di configurazione 112 che rappresenta un *client DCF*. Per esempio, gli attributi di dati possono consistere di 16 o 32 bit, in cui un dato numero di bit specifica l'indirizzo di uno dei client di dati di configurazione 112, e il carico utile può consistere di 16 o 32 bit. Per esempio, in varie forme di attuazione, il modulo di lettura di dati 1080 è configurato per leggere blocchi di 64 bit dalla memoria 104, in cui i primi 32 bit contengono gli attributi di dati (comprendendo l'indirizzo di un client di dati di configurazione) e i secondi 32 bit contengono i dati di configurazione da trasmettere all'indirizzo specificato negli attributi di dati.

Come descritto in precedenza, ciascun client di dati di configurazione/client DCF 112 può essere un circuito hardware, di solito comprendente un circuito combinatorio

configurato per memorizzare i dati ricevuti in un registro interno implementato, per es., con dei flip-flop/latch, permettendo con ciò di distribuire, tramite uno o più segnali interni generati in funzione dei dati memorizzati nel registro interno, i dati di configurazione ricevuti a varie parti del blocco (dei blocchi) hardware 110/150/156 associato (associati). Per esempio, come menzionato in precedenza, ciascun client di dati di configurazione 112 può avere associato un indirizzo univoco (cioè, univoco all'interno di ciascun sistema di elaborazione 10a) e analizza i dati trasmessi dal modulo di smistamento 1082 al fine di determinare se gli attributi di dati (attributi di Formato DCF) aggiuntivi contengono l'indirizzo associato al client di dati di configurazione 112.

In varie forme di attuazione, il modulo 108 può anche comprendere un modulo di controllo di stato 1084 configurato per gestire le varie fasi di configurazione del sistema di elaborazione 10a. Per esempio, in varie forme di attuazione, una volta che il sistema di elaborazione 10a è acceso, un modulo di reset 116 del sistema di elaborazione 10a può generare un segnale di reset RESET, che è usato per effettuare un reset dei vari componenti del sistema di elaborazione 10a. Per esempio, il segnale di reset RESET può corrispondere a un impulso di reset di un dato numero di cicli di clock, fornito ai blocchi 110 del sistema di elaborazione 10a. Per esempio, nella forma di attuazione considerata, il segnale di reset RESET può essere usato dai client di dati di configurazione 112 al fine di impostare il registro interno a un dato valore di reset.

Similmente, in risposta a un reset, il modulo di controllo di stato 1084 può attivare la fase di configurazione. Specificamente, durante la fase di

configurazione, il modulo di lettura di dati 1080 può leggere i dati di configurazione CD dalla memoria 104 e il modulo di smistamento 1082 può inviare i dati di configurazione CD ai vari client di dati di configurazione 112, sovrascrivendo con ciò i valori di reset.

Per esempio, in varie forme di attuazione, il modulo di smistamento 1082 può generare un segnale di dati DATA avente un dato numero di bit (corrispondenti ai bit del carico utile) contenenti i dati di configurazione da trasmettere a un dato client di dati di configurazione 112 e ulteriori segnali di controllo per selezionare il client di dati di configurazione 112 target. Per esempio, nella forma di attuazione considerata, il modulo di smistamento 1082 genera anche un segnale di indirizzo ADR che contiene l'indirizzo del client di dati di configurazione target 112 e opzionalmente un segnale di selezione di chip ("chip select") CS usato per segnalare che il segnale di indirizzo ADR e il segnale di dati DATA sono validi.

Per esempio, in varie forme di attuazione, il segnale di indirizzo ADR (e il segnale di chip select CS) possono essere forniti a un decodificatore 124 configurato per attivare uno dei client di dati di configurazione 112 in funzione del segnale di indirizzo ADD. Per esempio, nella forma di attuazione considerata, il decodificatore 124 può impostare un segnale di chip select CSa al fine di indicare che il client di dati di configurazione 112a dovrebbe leggere il segnale di dati DATA quando il segnale di indirizzo ADR corrisponde a un indirizzo assegnato al client di dati di configurazione 112a (e il segnale di chip select CS è impostato). Similmente, il decodificatore 124 può impostare un segnale di chip select CSb al fine di indicare che il client di dati di configurazione 112b dovrebbe leggere il

segnale di dati DATA quando il segnale di indirizzo ADR corrisponde a un indirizzo assegnato al client di dati di configurazione 112b (e il segnale di chip select CS è impostato), ecc.

Di conseguenza, come menzionato in precedenza, i dati di configurazione CD possono anche comprendere dati di configurazione di sicurezza usati per configurare le protezioni 150, come l'accesso esterno a un'interfaccia di debug o l'accesso (in lettura e/o in scrittura) a date locazioni di memoria, e le password di riferimento RK da memorizzare nel repository di password temporaneo 156.

Specificamente, in varie forme di attuazione, ciascun pezzo di dati di configurazione è inserito in un frame insieme all'identificatore/indirizzo di un client di dati di configurazione 112. Il circuito di configurazione hardware 108 legge tutti questi frame di dati di DCF programmati nella memoria non volatile 104 e li invia ai rispettivi client di dati di configurazione 112.

Di conseguenza, includendo la (le) password di riferimento RK nei frame di dati di DCF che hanno l'indirizzo del (dei) client di dati di configurazione 112c associato (associati) al repository di password temporaneo 156, la (le) password di riferimento RK può essere memorizzata (possono essere memorizzate) nel repository di password temporaneo 156.

Per esempio, come rappresentato nella Figura 8, il repository di password temporaneo 156 può comprendere uno o più slot PW0, PW1, …, ciascuno slot essendo atto a memorizzare una rispettiva password di riferimento RK. Inoltre, nella forma di attuazione considerata, un singolo client di dati di configurazione 112c è associato al repository di password temporaneo 156. In questo caso, una

pluralità di frame di DCF (ciascuno comprendente una rispettiva password di riferimento RK) può essere inviata in sequenza all'indirizzo del client di dati configurato 112c e, una volta che è ricevuta una password di riferimento RK, il repository di password temporaneo 156 può memorizzare la password di riferimento in un rispettivo slot PW0, PW1, … della memoria interna. Generalmente, il frame di DCF può anche includere un campo che indica il numero di slot in cui dovrebbe essere memorizzata la rispettiva password di riferimento RK.

Generalmente, a causa del fatto che i client di dati di configurazione 112 comprendono anche registri interni, questi registri possono anche essere usati direttamente come memoria del repository di password temporaneo 152. Per esempio, in questo caso, una pluralità di client di dati di configurazione 112c può essere associata al repository di password temporaneo 152, in cui ciascuno dei client di dati di configurazione 112c ha un rispettivo indirizzo (univoco). In questo caso, una pluralità di frame di DCF (ciascuno comprendente una rispettiva password di riferimento RK) può essere inviata in sequenza agli indirizzi dei client di dati di configurazione 112c.

Una volta che la fase di caricamento delle password è completata, le password di riferimento RK sono memorizzate nella memoria del repository di password temporaneo 152. Di conseguenza, non c'è alcuna necessità di accedere ulteriormente alle password di riferimento RK memorizzate nella memoria non volatile 104 a una richiesta di sfida ("challenge") di password. Di conseguenza, nella forma di attuazione considerata, la comunicazione non può essere spiata da altri blocchi del sistema di elaborazione 10a,

perché gli altri blocchi non sono operativi durante la fase di configurazione del sistema di elaborazione 10a.

Generalmente, grazie all'organizzazione dei dati di configurazione CD in pacchetti di dati, i dati di configurazione CD possono così comprendere almeno due sottoinsiemi di dati di configurazione, come:

- un primo gruppo di dati di configurazione (per es., dati di calibrazione) scritti dal produttore del sistema di elaborazione 10a, per es., il fabbricante del chip; e
- un secondo gruppo di dati di configurazione scritti durante uno stadio successivo, come dati di configurazione scritti dallo sviluppatore del firmware e/o da un integratore del sistema, come il produttore di una Unità di Controllo del Motore (ECU).

Per esempio, in questo caso, i dati di configurazione di sicurezza inclusi nel primo gruppo di dati di configurazione possono anche permettere di impostare i diritti di accesso alle locazioni di memoria, in cui è memorizzato il primo gruppo di dati di configurazione. Per esempio, in questo modo, il primo gruppo di dati di configurazione non può essere sovrascritto e/o l'interfaccia di memoria può inibire un accesso in lettura al primo gruppo di dati di configurazione (per es., da parte dell'unità di elaborazione 102). Per contro, i dati di configurazione di sicurezza inclusi nel secondo gruppo di dati di configurazione possono essere usati per configurare il comportamento dei blocchi 110 da un punto di vista funzionale, per es., al fine di abilitare o disabilitare l'interfaccia di debug, ecc. Così, anche in questo caso, una volta che l'interfaccia di debug è disattivata, il secondo gruppo di dati di configurazione non può essere sovrascritto o letto. Similmente, la (le) password di riferimento usata

(usate) per sbloccare le protezioni può essere configurata (possono essere configurate) insieme al primo gruppo e/o al secondo gruppo di dati di configurazione. Per esempio, il primo gruppo può contenere una password di riferimento per effettuare operazioni di accesso a locazioni di memoria protette in lettura e/o in scrittura e il secondo gruppo può contenere una password di riferimento per abilitare di nuovo l'interfaccia di debug.

Per contro, i dati del ciclo di vita LCD indicano il ciclo di vita del prodotto. Il ciclo di vita è una firma permanente scritta in una memoria non volatile, che determina lo stadio del sistema di elaborazione 10a durante la sua durata di vita ("life-time"). Per esempio, il ciclo di vita può essere codificato con una sequenza di bit. Per esempio, in varie forme di attuazione, la sequenza di bit LCD può indicare uno degli stadi seguenti:

- "produzione" (LC1), quando il sistema di elaborazione 10a, per es., un microcontrollore, è nella fabbrica di chip;
- "consegna al cliente" (LC2), quando il sistema di elaborazione 10a è stato spedito al cliente di 1° livello (per es., un produttore di un'unità di controllo del motore);
- "produzione OEM" (LC3), quando il dispositivo è stato spedito a un cliente di livello successivo (per es., un fabbricante di automobili);
- "in campo" (LC4), quando il dispositivo è installato nel prodotto finale (per es., in un'automobile venduta sul mercato);
- "analisi guasti" (LC5), quando il dispositivo è rispedito al produttore del sistema di elaborazione 10a o allo sviluppatore del software a scopi di diagnostica.

In varie forme di attuazione, questa sequenza di bit è memorizzata in locazioni di memoria riservate della memoria

non volatile 104 o in una memoria non volatile 126 separata, come una memoria programmabile una sola volta. In varie forme di attuazione, i dati del ciclo di vita LCD sono scritti in modo tale che, una volta che è raggiunto un certo stadio, non sia possibile ritornare indietro a uno stadio precedente, cioè, il ciclo di vita può soltanto avanzare. Per esempio, questo può essere implementato con una codifica "one-hot", in cui un fusibile è bruciato ogni volta che è stato raggiunto un dato stadio. Per esempio, l'avanzamento del ciclo di vita allo stadio successivo può essere fatto dall'entità che possiede il dispositivo nello stadio del ciclo di vita corrente (per es., il produttore del chip farà avanzare il ciclo di vita quando è spedito allo stadio di consegna al cliente; il cliente di 1° livello farà avanzare il ciclo di vita quando è spedito allo stadio di produzione OEM, ecc.).

Come rappresentato nella Figura 8, in varie forme di attuazione, il circuito di configurazione hardware 108 può anche essere configurato per leggere la sequenza di bit/i dati del ciclo di vita dalla memoria 126 (o 104), memorizzare i dati del ciclo di vita in un registro 128 e il segnale LCD può corrispondere ai dati del ciclo di vita memorizzati in questo registro. Per esempio, il circuito di configurazione hardware 108 può memorizzare i dati del ciclo di vita in un registro:

- memorizzando i dati del ciclo di vita in un registro del circuito di configurazione 108, cioè, il registro 128 può essere integrato nel circuito di configurazione 108; e/o

- trasferendo i dati del ciclo di vita a uno o più client di dati di configurazione dedicati 112, cioè, il registro 128 può essere integrato in uno o più client di dati di configurazione 112.

Per esempio, questa soluzione può essere usata quando i dati del ciclo di vita sono memorizzati nella memoria non volatile 104 e/o quando i dati del ciclo di vita possono essere sovrascritti a scopi di test/debug.

Generalmente, il circuito di configurazione 108 può anche essere configurato per decodificare la sequenza di bit del ciclo di vita letta dalla memoria 126 (o 104). Per esempio, la sequenza di bit del ciclo di vita letta dalla memoria può corrispondere a una sequenza di bit codificata (per es., "one-hot"), e il segnale LCD può corrispondere a una sequenza codificata binaria che indica un valore numerico associato al rispettivo stadio del ciclo di vita. Generalmente, in questo caso, la sequenza di bit codificata o la sequenza di bit decodificata può essere memorizzata nel registro 128, cioè, la decodifica può essere effettuata prima o dopo la memorizzazione dei dati nel registro 128.

Di conseguenza, in varie forme di attuazione, il sistema di elaborazione 10a comprende registri usati per memorizzare informazioni rilevanti per la sicurezza, in particolare uno o più tra:

- i registri configurati per memorizzare i dati di configurazione usati per abilitare o disabilitare i circuiti di protezione 150, come i registri dei client di dati di configurazione 112b; e/o

- i registri configurati per memorizzare la (le) password di riferimento usata (usate) per sovrascrivere le protezioni fatte rispettare da uno o più dei circuiti di protezione 150, come i registri dei client di dati di configurazione 112c; e/o

- il registro (i registri) 128 configurato (configurati) per memorizzare i dati del ciclo di vita LCD.

Gli inventori hanno osservato che tali registri dovrebbero così essere protetti al fine di evitare che i registri possano essere sovrascritti intenzionalmente o non intenzionalmente. Per esempio, a questo scopo, la Pubblicazione della Domanda di Brevetto Statunitense US 2019/0227747 A1 descrive forme di attuazione di client di dati di configurazione 112, in cui il client di dati di configurazione può essere configurato per permettere o inibire selettivamente la sovrascrittura di dati di configurazione già memorizzati in funzione di almeno un segnale di identificazione del tipo. Questo documento è così incorporato qui tramite citazione per possibili forme di attuazione dei client di dati di configurazione 112.

Il meccanismo appena descritto permette così di decidere se un dato pacchetto di dati di configurazione può sovrascrivere dati di configurazione precedenti, già memorizzati nello stesso client 112, per esempio al fine di evitare che protezioni già attivate possano essere disattivate di nuovo mediante un pacchetto di DCF successivo indirizzato allo stesso client di dati di configurazione 112. Tuttavia, una tale protezione non copre tutti i possibili attacchi di manomissione. Specificamente, tali attacchi di manomissione si riferiscono a tecniche che intendono modificare lo stato di bit (per esempio, con attacchi elettromagnetici) di un flip-flop/latch, di solito che intendono rimuovere la protezione programmata o semplicemente ripristinare lo stato di protezione di bit di default, che di solito corrisponde allo stato non protetto.

La Figura 9 rappresenta a questo riguardo una forma di attuazione di un sistema di elaborazione 10a modificato.

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

- un circuito di protezione 150 configurato per controllare l'accesso a una rispettiva risorsa 110 in funzione di dati di configurazione, indicati in seguito come dati di configurazione CDb;

- una pluralità di client di dati di configurazione 112, in cui almeno un client di dati di configurazione 112b è configurato per memorizzare i dati di configurazione CDb per il circuito di protezione 150;

- una memoria non volatile 104 configurata per memorizzare i dati di configurazione CD per uno o più della pluralità di client di dati di configurazione 112, per es., sotto forma di pacchetti di dati, in cui ciascun pacchetto di dati comprende anche un indirizzo di un rispettivo client di dati di configurazione 112; e

- un circuito di configurazione hardware 108 configurato per leggere i dati di configurazione CD dalla memoria non volatile 104 e memorizzare i dati di configurazione nei client di dati di configurazione 112.

Per esempio, nella forma di attuazione considerata, ciascun client di dati di configurazione 112 comprende un registro configurato per memorizzare un dato numero N di bit, come 32 o 64 bit. Specificamente, la Figura 9 rappresenta a questo riguardo un singolo elemento di memorizzazione 113 del client di dati di configurazione 112, in cui l'elemento di memorizzazione 113 comprende un latch o un flip-flop 1122 configurato per memorizzare un singolo bit. Di conseguenza, in varie forme di attuazione, ciascun client di dati di configurazione 112 comprende N elementi di memorizzazione 113.

Come menzionato in precedenza, in varie forme di attuazione, un dato client di dati di configurazione 112 può fornire dati di configurazione a vari circuiti 110 e/o

circuiti di protezione 150, cioè, i dati di configurazione CDb possono corrispondere ai dati forniti da un sottoinsieme degli elementi di memorizzazione 113 di un dato client di dati di configurazione 112. In aggiunta o in alternativa, in varie forme di attuazione, un circuito 110 e/o circuito di protezione 150 possono ricevere dati di configurazione da vari client di dati di configurazione 112, cioè, un dato circuito di protezione 150 può ricevere dati di configurazione CDb dagli elementi di memorizzazione 113 di almeno due client di dati di configurazione 112. Generalmente, i dati di configurazione CDb possono così corrispondere a uno o più bit che indicano se il circuito di protezione 150 dovrebbe fare rispettare una o più regole di sicurezza.

Di conseguenza, in varie forme di attuazione, ciascun client di dati di configurazione 112 è configurato per ricevere una richiesta di scrittura comprendente dati da scrivere negli elementi di memorizzazione 113 del client di dati di configurazione 112 e per memorizzare, in risposta alla richiesta di scrittura, i dati ricevuti nei latch o nei flip-flop 1122. Per esempio, la richiesta di scrittura può corrispondere al segnale di dati DATA e al segnale di chip select CS descritti precedentemente, o a un segnale di abilitazione di scrittura simile. A questo riguardo, sebbene non rappresentato nella Figura 9, l'elemento di memorizzazione 113 può anche essere configurato per eseguire selettivamente la richiesta di scrittura in funzione delle informazioni di identificazione del tipo menzionate in precedenza, per es., al fine di eseguire solo una prima richiesta di scrittura e di inibire quindi ulteriori operazioni di scrittura nel latch o nel flip-flop 1122, assicurando con ciò che i dati di configurazione memorizzati

non possano essere sovrascritti da ulteriori richieste di scrittura.

A questo riguardo, in varie forme di attuazione, ciascun client di dati di configurazione 112 è configurato per resettare il contenuto dell'elemento di memorizzazione 113, in particolare dei latch o dei flip-flop 1122, a un valore di reset/default RV in risposta a un segnale di reset RESET. Per esempio, come menzionato, un tale segnale di reset RESET può essere generato da un circuito di reset 116, per es., configurato per generare un impulso/innesco ("trigger") nel segnale di reset RESET quando il sistema di elaborazione 10a è acceso e/o in risposta ad altri eventi. In alternativa, il segnale di reset RESET può anche essere fornito dai circuiti di configurazione 108, per es., dal circuito di controllo di stato 1084.

Per esempio, nella forma di attuazione considerata, il segnale di reset RESET è fornito a un multiplexer 1120, che è configurato per memorizzare nel latch o nel flip-flop 1122 i dati forniti dal circuito di configurazione 108, come un dato bit del segnale DATA menzionato precedentemente, o un valore di reset RV. Di conseguenza, al fine di memorizzare i dati nel latch o nel flip-flop 1122, l'elemento di memorizzazione può essere configurato per memorizzare il segnale fornito dal multiplexer 1120 in risposta alla richiesta di scrittura (come indicato, per es., dal segnale di chip select CS) o in risposta al segnale di reset.

Generalmente, il valore di reset RV può corrispondere al livello logico 1 o al livello logico 0, in base al fatto che il rispettivo bit dei dati di configurazione CDb dovrebbe essere impostato alto o basso di default.

In varie forme di attuazione, gli elementi di memorizzazione 113, in particolare almeno gli elementi di

memorizzazione 113 disposti per memorizzare informazioni rilevanti per la sicurezza, sono così protetti da possibili attacchi di manomissione.

Specificamente, in varie forme di attuazione, uno o più degli elementi di memorizzazione 113 di un dato client di dati di configurazione 112, come un client di dati di configurazione 112b, che forniscono rispettivi uno o più bit di dati di configurazione CDb a un circuito di protezione 150, comprendono in aggiunta al latch o al flip-flop 1122 un ulteriore latch o flip-flop 1124.

Specificamente, in varie forme di attuazione, i latch o i flip-flop 1122 e 1124 sono disposti in stretta prossimità all'interno del circuito integrato 30 del sistema di elaborazione 10a. In effetti, gli inventori hanno osservato che, in questo caso, è probabile che un attacco di manomissione imposterà a 0 o 1 entrambi i latch o i flip-flop 1122 e 1124 fisici, ma sarà quasi impossibile imporre un livello logico differente.

Di conseguenza, al fine di rilevare un possibile attacco di manomissione, l'elemento di memorizzazione 113 comprende anche un inverter/una porta logica NOT 1126 configurata per memorizzare nel latch o nel flip-flop 1124 la versione invertita del valore logico memorizzato nel registro 1122, per es., memorizzando nel latch o nel flip-flop 1124 la versione invertita del bit fornito dal multiplexer 1120. Inoltre, l'elemento di memorizzazione comprende una porta logica XOR 1128 che riceve in ingresso i valori dei bit memorizzati nei latch o nei flip-flop 1122 e 1124 e che fornisce in uscita un segnale di manomissione TAMP.

Di conseguenza, in varie forme di attuazione, l'elemento di memorizzazione è configurato per memorizzare un dato valore di bit (DATA o RV) nel latch o nel flip-flop

1122 e il rispettivo valore di bit (DATA o RV) invertito nel latch o nel flip-flop 1124. Inoltre, l'elemento di memorizzazione 113 è configurato per asserire il segnale di manomissione TAMP quando i latch o i flip-flop 1122 e 1124 sono impostati allo stesso valore.

Di conseguenza, in varie forme di attuazione, l'uno o più elementi di memorizzazione 113 di un dato client di dati di configurazione 112, che forniscono rispettivi uno o più bit di dati di configurazione CDb a un circuito di protezione 150, forniscono anche i rispettivi segnali di manomissione TAMP al circuito di protezione 150. Di conseguenza, in questo caso, il circuito di protezione 150 può essere configurato per controllare l'accesso a una rispettiva risorsa 110 non solo in funzione dei bit dei dati di configurazione CDb, ma anche in funzione dei rispettivi segnali di manomissione TAMP.

Per esempio, nel caso in cui il circuito di protezione 150 sia configurato per abilitare o disabilitare l'accesso al circuito 110 associato in funzione dei dati di configurazione CDb, per es., per abilitare l'accesso quando un dato bit dei dati di configurazione CDb è impostato al rispettivo valore di reset RV (per es., basso) e per disabilitare l'accesso quando il dato bit dei dati di configurazione CDb è impostato al valore invertito del valore di reset RV (per es., alto), il circuito di protezione 150 può disabilitare in ogni caso l'accesso quando il rispettivo segnale di manomissione TAMP è asserito.

Tuttavia, in generale, il circuito di protezione 150 può anche gestire l'accesso a una pluralità di circuiti 110 o di aree di memoria, come l'accesso di un'interfaccia di debug 50 a una pluralità di circuiti 110 e/o di aree di memoria. Per esempio, in questo caso, i dati di

configurazione CDb possono comprendere uno o più bit per abilitare/disabilitare l'accesso a ciascuno dei sotto-circuiti o a ciascuna delle aree di memoria. Di conseguenza, in varie forme di attuazione, quando un dato segnale di manomissione TAMP è asserito, il circuito di protezione 150 può attivare una data configurazione (per es., indicando che l'accesso dovrebbe essere disabilitato) soltanto per il rispettivo circuito 110 o la rispettiva area di memoria, un sottoinsieme dei circuiti e/o delle aree di memoria, o perfino tutti i circuiti 110 e/o tutte le aree di memoria gestiti dal circuito di protezione 150.

Per esempio, la Figura 10 rappresenta una forma di attuazione in cui il sistema di elaborazione 10a è configurato per attivare una data configurazione soltanto per il rispettivo bit di dati di configurazione CDb.

Specificamente, nella forma di attuazione considerata, il bit di dati di configurazione CDb fornito dal rispettivo latch o flip-flop 1122 è fornito a un multiplexer 1130. Il multiplexer 1130 riceve anche il rispettivo segnale di manomissione TAMP e un valore TV indicativo della configurazione da usare nel caso di un attacco di manomissione. Di conseguenza, nella forma di attuazione considerata, il multiplexer 1130 è configurato per fornire un bit di dati di configurazione CDb' al circuito di protezione 150, in cui il bit CDb' corrisponde:

- quando il segnale di manomissione TAMP è deasserito, al bit di dati di configurazione CDb fornito dal rispettivo latch o flip-flop 1122; o

- quando il segnale di manomissione TAMP è deasserito, al bit TV.

Generalmente, il multiplexer 1130 (e similmente il multiplexer 1120) può anche essere sostituito con un

qualsiasi altro circuito logico combinatorio adeguato. Per esempio, nel caso in cui il segnale TV sia impostato alto, il multiplexer 1122 può essere sostituito con una porta logica OR che riceve in ingresso il bit di dati di configurazione CDb e il segnale di manomissione TAMP.

Per esempio, il circuito logico combinatorio 1130 può essere:

- integrato nell'elemento di memorizzazione 113, per cui l'elemento di memorizzazione gestisce già la protezione da manomissione per il rispettivo bit e fornisce una data configurazione TV predeterminata nel caso di un attacco di manomissione;

- integrato nel circuito di protezione 150;

- esterno rispetto all'elemento di memorizzazione 113 e al circuito di protezione 150.

Inoltre, in linea con la descrizione precedente, un tale circuito logico combinatorio 1130 può essere configurato per ricevere i segnali di manomissione TAMP da una pluralità di elementi di memorizzazione 113.

Per esempio, questo è rappresentato anche nella Figura 11. Specificamente, la Figura 11 rappresenta una forma di attuazione, in cui il client di dati di configurazione 112 fornisce una pluralità di bit di dati di configurazione a un dato circuito associato.

Per esempio, questo si applica al client di dati di configurazione 112c che fornisce una o più chiavi di riferimento RK al circuito di verifica di password 152.

Di conseguenza, anche in questo caso, l'elemento di memorizzazione 113 descritto in precedenza (con il latch 1124 e la porta logica XOR 1128 aggiuntivi) può essere usato per fornire, per ciascun bit di dati di configurazione (come

fornito dai rispettivi latch 1122), anche un rispettivo segnale di manomissione TAMP.

Per esempio, in questo caso, il circuito di verifica di password 152 può ricevere una data chiave di riferimento RK da uno o più client di dati di configurazione 112c e i rispettivi segnali di manomissione TAMP.

Specificamente, in varie forme di attuazione, il circuito di verifica di password 152 è configurato per disabilitare l'operazione di verifica di password quando almeno uno dei segnali di manomissione ricevuti TAMP è asserito. In effetti, quando uno dei segnali di manomissione TAMP è asserito, la rispettiva chiave di riferimento RK non è più valida.

Di conseguenza, in varie forme di attuazione, anche se il comando di verifica di password VPW fornisce una password corrispondente alla chiave di riferimento RK, il circuito di verifica di password 152 è configurato per mantenere deasserito il segnale di sovrascrittura OW.

Di conseguenza, in questo caso, il circuito logico combinatorio configurato per combinare una pluralità di segnali di manomissione TAMP sarebbe implementato all'interno del circuito di verifica di password 152.

Tuttavia, la Figura 11 rappresenta schematicamente anche un circuito logico combinatorio 1502, come una porta logica OR, configurato per generare un segnale di manomissione combinato TAMP' combinando una pluralità di segnali di manomissione TAMP forniti da un dato client di dati di configurazione 112 e/o da una pluralità di client di dati di configurazione 112.

Per esempio, in questo modo, un circuito di protezione 150 può ricevere un segnale di manomissione combinato TAMP', che è asserito quando almeno uno dei segnali di manomissione

TAMP associati (come ricevuti dal rispettivo circuito logico combinatorio 1502) è asserito.

Per esempio, in questo modo, il segnale di manomissione combinato TAMP' può essere asserito:

- come rappresentato nella Figura 9, quando un segnale di manomissione TAMP associato a un dato bit di dati di configurazione CDb gestito dal circuito di protezione 150 è asserito; e/o

- come rappresentato nella Figura 11, quando un segnale di manomissione TAMP associato a una password di riferimento RK usata per sovrascrivere una o più protezioni gestite dal circuito di protezione 150 è asserito.

Come menzionato in precedenza, uno o più dei circuiti di protezione 150 e/o il circuito di verifica di password 152, può essere configurato per funzionare anche in funzione di dati del ciclo di vita LCD.

Di conseguenza, le soluzioni precedenti applicate ai dati di configurazione CDb e/o alla chiave di riferimento RK possono anche essere usate per i dati del ciclo di vita.

Per esempio, questo è rappresentato schematicamente nella Figura 12, in cui il registro 128 descritto precedentemente configurato per memorizzare i dati del ciclo di vita LCD è sostituito con un insieme di elementi di memorizzazione 113.

Di conseguenza, in questo caso l'elemento di memorizzazione 113 comprende un latch o un flip-flop 1122 e un ulteriore latch o flip-flop 1124, in cui i dati del ciclo di vita LCD corrispondono ai bit memorizzati nei latch o nei flip-flop 1122, e in cui l'elemento di memorizzazione 113 è configurato per ricevere una richiesta di scrittura comprendente un bit di dati e per memorizzare, in risposta alla richiesta di scrittura, il bit di dati ricevuto nel

rispettivo latch o flip-flop 1122 e la versione invertita del bit di dati dei dati ricevuti nel rispettivo latch o flip-flop 1124. Anche in questo caso, l'elemento di memorizzazione 113 può gestire un segnale di reset RESET al fine di resettare il contenuto del latch o del flip-flop 1122.

Inoltre, l'elemento di memorizzazione 113 è configurato per asserire un segnale di manomissione TAMP per il rispettivo latch o flip-flop 1122 quando i rispettivi latch o flip-flop 1122 e 1124 memorizzano lo stesso livello logico.

Per esempio, nella forma di attuazione considerata, i segnali di manomissione TAMP associati ai dati del ciclo di vita LCD sono forniti al circuito di protezione 150 (come descritto anche con riferimento alla Figura 9). Tuttavia, in modo simile alle forme di attuazione descritte con riferimento alla Figura 10 o 11, il circuito di protezione 150 può ricevere:

- dati del ciclo di vita predeterminati dati, quando almeno uno dei segnali di manomissione TAMP associato ai dati del ciclo di vita LCD è asserito, come dati del ciclo di vita che indicano uno stadio del ciclo di vita in cui è applicato il più alto livello di sicurezza, come lo stadio in campo; e/o

- un segnale di manomissione combinato TAMP' generato combinando i segnali di manomissione TAMP associati ai bit dei dati del ciclo di vita LCD.

In varie forme di attuazione, i segnali di manomissione TAMP e/o i segnali di manomissione combinati TAMP' possono anche essere forniti a uno o più circuiti ulteriori all'interno del circuito di elaborazione 10a, come un microprocessore 1020 e/o un circuito di gestione degli errori. Per esempio, in varie forme di attuazione, un segnale

di manomissione combinato TAMP' è fornito come un segnale di interruzione ("interrupt") e/o un bit di stato di registro al microprocessore 1020, e il microprocessore 1020 può essere atto a leggere anche il contenuto dei segnali di manomissione associati.

Di conseguenza, nelle forme di attuazione descritte in precedenza, il sistema di elaborazione 10a comprende un circuito hardware 110, come un controllore di memoria 100 o una risorsa/periferica 106, e un circuito di elaborazione digitale 102 e/o un'interfaccia di debug 50 configurati per fornire un comando di controllo CMD per controllare il funzionamento del circuito hardware 110.

In varie forme di attuazione, il sistema di elaborazione 102 comprende anche un circuito di protezione 150 configurato per ricevere il comando di controllo CMD e per inoltrare selettivamente il comando di controllo CMD al circuito hardware 110 in funzione di uno o più segnali di controllo. Per esempio, l'uno o più segnali di controllo possono corrispondere ai dati di configurazione CDb, ai dati del ciclo di vita LCD e/o al segnale di sovrascrittura OW.

Specificamente, in varie forme di attuazione, il sistema di elaborazione 10a comprende anche uno o più elementi di memorizzazione 113, in cui ciascun elemento di memorizzazione 113 comprende un rispettivo latch o flip-flop 1122, e in cui l'uno o più segnali di controllo sono generati in base al contenuto dell'uno o più latch o flip-flop 1122. Di conseguenza, ciascun segnale di controllo può corrispondere al segnale fornito da un rispettivo latch o flip-flop 1122, per es., nel caso dei dati di configurazione CDb e/o dei dati del ciclo di vita LCD, o può essere generato mediante operazioni logiche più complesse, per es., nel caso

del segnale di sovrascrittura OW generato dal circuito di verifica di password 152.

Specificamente, in varie forme di attuazione, ciascun elemento di memorizzazione 113 comprende un ulteriore latch o flip-flop 1124 ed è configurato per ricevere una richiesta di scrittura comprendente un bit di dati e per memorizzare, in risposta alla richiesta di scrittura, il bit di dati ricevuto nel rispettivo latch o flip-flop 1122 e la versione invertita del bit di dati dei dati ricevuti nel rispettivo latch o flip-flop 1124. In varie forme di attuazione, l'elemento di memorizzazione 113 può anche ricevere un segnale di reset RESET e, in risposta al segnale di reset RESET, può resettare il contenuto del latch o del flip-flop 1122 a un dato valore di reset RV e il contenuto del latch o del flip-flop 1124 alla versione invertita del valore di reset RV.

Di conseguenza, in varie forme di attuazione, il sistema di elaborazione comprende una memoria non volatile configurata per memorizzare i bit di dati (cioè, i dati di configurazione e/o la sequenza di bit di dati del ciclo di vita) e un circuito di configurazione hardware 108 configurato per leggere i bit di dati dalla memoria non volatile e generare le richieste di scrittura al fine di memorizzare i bit di dati negli elementi di memorizzazione 113.

Specificamente, in varie forme di attuazione, l'elemento di memorizzazione 113 è configurato per asserire un segnale di manomissione TAMP per il rispettivo latch o flip-flop 1122 quando i rispettivi latch o flip-flop 1122 e 1124 memorizzano lo stesso livello logico e per deasserire un segnale di manomissione TAMP per il rispettivo latch o

flip-flop 1122 quando i rispettivi latch o flip-flop 1122 e 1124 memorizzano livelli logici differenti.

Di conseguenza, in varie forme di attuazione, il sistema di elaborazione 10a è configurato in modo tale che il circuito di protezione 150 inoltri il comando di controllo CMD al circuito hardware 110 anche in funzione dei segnali di manomissione TAMP. Per esempio, a questo scopo, il circuito di protezione 150 può:

- ricevere direttamente i segnali di manomissione TAMP; e/o

- uno o più dei segnali di controllo possono essere generati non soltanto in base al contenuto dell'uno o più latch o flip-flop 1122 ma anche in funzione dei segnali di manomissione TAMP.

In generale, sebbene le forme di attuazione precedenti siano relative principalmente ai dati di configurazione relativi alla sicurezza, gli elementi di memorizzazione 113 possono essere usati per proteggere anche altri dati, per es., al fine di imporre dati di configurazione di default nel caso di un attacco di manomissione (come rappresentato nella Figura 10).

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:

- una pluralità di elementi di memorizzazione (113), in cui ciascun elemento di memorizzazione (113) comprende un latch o un flip-flop (1122) ed è configurato per ricevere una richiesta di scrittura comprendente un bit di dati e per memorizzare il bit di dati ricevuto in detto latch o flip-flop (1122);

- una memoria non volatile (104; 126) configurata per memorizzare bit di dati (CD, LCD) per detta pluralità di elementi di memorizzazione (113);

- un circuito di configurazione hardware (108) configurato per leggere detti bit di dati da detta memoria non volatile (104; 126) e generare richieste di scrittura al fine di memorizzare detti bit di dati in detti elementi di memorizzazione (113); e

- un circuito hardware (110, 150, 152, 1130, 1502) configurato per cambiare operazione in funzione del livello logico memorizzato nel latch o nel flip-flop (1122) di un primo elemento di memorizzazione (113) di detta pluralità di elementi di memorizzazione (113);

in cui detto primo elemento di memorizzazione (113) comprende un ulteriore latch o flip-flop (1124) ed è configurato per memorizzare, in risposta a detta richiesta di scrittura, la versione invertita (1126) di detto bit di dati ricevuto in detto ulteriore latch o flip-flop (1124), e in cui detto primo elemento di memorizzazione (113) comprende un circuito logico combinatorio (1128) configurato per:

- confrontare il livello logico memorizzato in detto latch o flip-flop (1122) di detto primo elemento di

memorizzazione (113) con il livello logico memorizzato in detto ulteriore latch o flip-flop (1122) di detto primo elemento di memorizzazione (113),

- deasserire un primo segnale di manomissione (TAMP) associato a detto primo elemento di memorizzazione (113) quando detti livelli logici sono differenti, e

- asserire detto primo segnale di manomissione (TAMP) quando i livelli logici sono gli stessi;

e in cui detto circuito hardware (110, 150, 152, 1130, 1502) è configurato per cambiare operazione anche in funzione di detto primo segnale di manomissione (TAMP).

2. Sistema di elaborazione (10a) secondo la Rivendicazione 1, comprendente un microprocessore (102) e/o un'interfaccia di debug (50) configurati per fornire un comando di controllo (CMD) per controllare il funzionamento di detto circuito hardware (110, 150, 152, 1130, 1502), e in cui detto circuito hardware (110, 150, 152, 1130, 1502) comprende un circuito di protezione (150, 1130) configurato per ricevere detto comando di controllo (CMD) e per eseguire selettivamente detto comando di controllo (CMD) in funzione del livello logico memorizzato nel latch o nel flip-flop (1122) di detto primo elemento di memorizzazione (113) e di detto primo segnale di manomissione (TAMP).

3. Sistema di elaborazione (10a) secondo la Rivendicazione 2, in cui detto circuito di protezione (150, 1130) è configurato per:

- eseguire detto comando di controllo (CMD) quando il latch o il flip-flop (1122) di detto primo elemento di memorizzazione (113) ha memorizzato un primo livello logico

e detto primo segnale di manomissione (TAMP) è deasserito, e

- inibire l'esecuzione di detto comando di controllo (CMD) quando il latch o il flip-flop (1122) di detto primo elemento di memorizzazione (113) ha memorizzato un secondo livello logico o detto primo segnale di manomissione (TAMP) è asserito.

4. Sistema di elaborazione (10a) secondo la Rivendicazione 2 o la Rivendicazione 3, in cui detto circuito di protezione (150, 1130) è configurato per eseguire selettivamente detto comando di controllo (CMD) in funzione di un segnale di controllo (CDb), e in cui detto circuito hardware (110, 150, 152, 1130, 1502) o detto primo elemento di memorizzazione (113) comprende un circuito logico combinatorio (1130) configurato per:

- determinare se detto primo segnale di manomissione (TAMP) è asserito,

- in risposta alla determinazione che detto primo segnale di manomissione (TAMP) è deasserito, impostare detto primo segnale di controllo (CD) al valore logico memorizzato nel latch o nel flip-flop (1122) di detto primo elemento di memorizzazione (113), e

- in risposta alla determinazione che detto primo segnale di manomissione (TAMP) è asserito, impostare detto primo segnale di controllo (CD) a un valore di manomissione (TV) predeterminato.

5. Sistema di elaborazione (10a) secondo una qualsiasi delle rivendicazioni precedenti, in cui detto circuito di protezione (150) è configurato per gestire l'accesso a una pluralità di sotto-circuiti e/o di aree di memoria, e in cui

a ciascun sotto-circuito e/o a ciascuna area di memoria è associato almeno un rispettivo primo elemento di memorizzazione (113), e in cui detto circuito di protezione (150, 1130) è configurato per inibire l'esecuzione di detto comando di controllo (CMD) quando almeno uno dei primi segnali di manomissione (TAMP) forniti da detta pluralità di primi elementi di memorizzazione (113) è asserito.

6. Sistema di elaborazione (10a) secondo una qualsiasi delle rivendicazioni precedenti da 2 a 5, in cui detto circuito di protezione (150) è configurato per eseguire detto comando di controllo (CMD) quando un segnale di sovrascrittura (OW) è asserito, e in cui detto circuito hardware (110, 150, 152, 1130, 1502) comprende un circuito di verifica di password (152) configurato per:

- ricevere un comando di verifica di password (VPW) da detto microprocessore (102) e/o da detta interfaccia di debug (50), detto comando di verifica di password (VPW) comprendendo una password, e
- confrontare detta password con una chiave di riferimento (RK), in cui detta chiave di riferimento (RK) è determinata in funzione dei livelli logici memorizzati nel latch o nel flip-flop (1122) di una pluralità di secondi elementi di memorizzazione (113) di detta pluralità di elementi di memorizzazione (113), e
- asserire detto segnale di sovrascrittura (OW) quando detta password corrisponde a detta chiave di riferimento (RK).

7. Sistema di elaborazione (10a) secondo la Rivendicazione 6, in cui ciascuno di detti secondi elementi di memorizzazione (113) comprende un ulteriore latch o flip-

flop (1124) e un circuito logico combinatorio (1128) configurato per asserire selettivamente un secondo segnale di manomissione (TAMP) confrontando il livello logico memorizzato nel latch o nel flip-flop (1122) del rispettivo secondo elemento di memorizzazione (113) con il livello logico memorizzato nell'ulteriore latch o flip-flop (1124) del rispettivo secondo elemento di memorizzazione (113).

8. Sistema di elaborazione (10a) secondo la Rivendicazione 7, in cui detto circuito di verifica di password (152) è configurato per:

- asserire detto segnale di sovrascrittura (OW) quando detta password corrisponde a detta chiave di riferimento (RK) e detti secondi segnali di manomissione (TAMP) forniti da detti secondi elementi di memorizzazione (113) sono deasseriti, e
- deasserire detto segnale di sovrascrittura (OW) quando detta password non corrisponde a detta chiave di riferimento (RK) o almeno uno di detti secondi segnali di manomissione (TAMP) forniti da detti secondi elementi di memorizzazione (113) è asserito.

9. Sistema di elaborazione (10a) secondo la Rivendicazione 7 o la Rivendicazione 8, in cui detto circuito di protezione (150, 1130) è configurato per:

- inibire l'esecuzione di detto comando di controllo (CMD) quando almeno uno di detti secondi segnali di manomissione (TAMP) forniti da detti secondi elementi di memorizzazione (113) è asserito.

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

11. Dispositivo, come un veicolo, comprendente una pluralità di sistemi di elaborazione (10a) secondo una qualsiasi delle precedenti Rivendicazioni da 1 a 9, in cui detti sistemi di elaborazione (10a) sono connessi mediante un sistema di comunicazione (20).

12. Procedimento di funzionamento di un sistema di elaborazione (10a) secondo una qualsiasi delle precedenti Rivendicazioni da 1 a 9, comprendente:

- memorizzare bit di dati (CD, LCD) per la pluralità di elementi di memorizzazione (113) di detto sistema di elaborazione (10a) nella memoria non volatile (104; 126) di detto sistema di elaborazione (10a); e
- accendere detto sistema di elaborazione (10a), per cui:
    - il circuito di configurazione hardware (108) di detto sistema di elaborazione (10a) legge detti bit di dati da detta memoria non volatile (104; 126) e genera richieste di scrittura al fine di memorizzare detti bit di dati negli elementi di memorizzazione (113) di detto sistema di elaborazione (10a); e
    - il primo elemento di memorizzazione (113) di detto sistema di elaborazione (10a):

    a) confronta il livello logico memorizzato nel latch o nel flip-flop (1122) del primo elemento di memorizzazione (113) con il livello logico memorizzato nell'ulteriore latch o flip-flop (1122) del primo elemento di memorizzazione (113),

b) deasserisce il primo segnale di manomissione (TAMP) associato al primo elemento di memorizzazione (113) quando i livelli logici sono differenti, e

c) asserisce il primo segnale di manomissione (TAMP) quando i livelli logici sono gli stessi.

FIG. 1

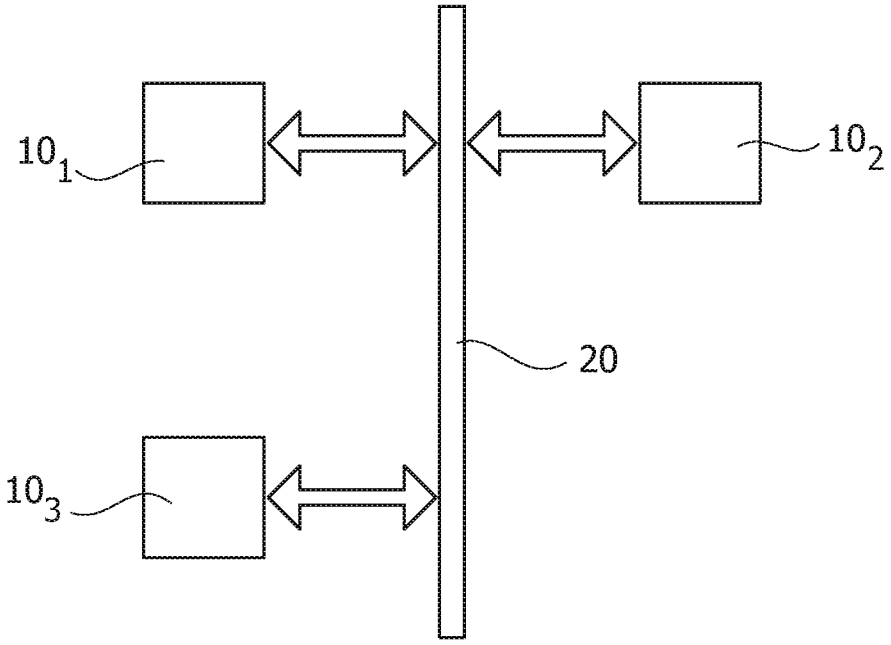


FIG. 2

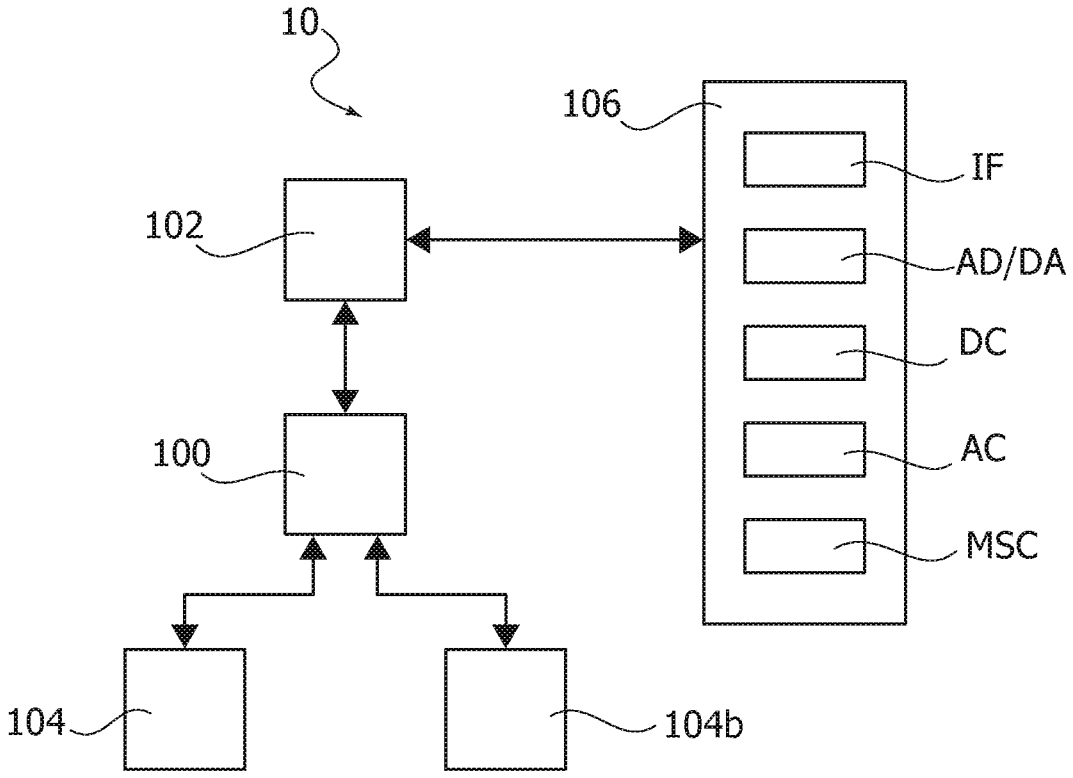


FIG. 3

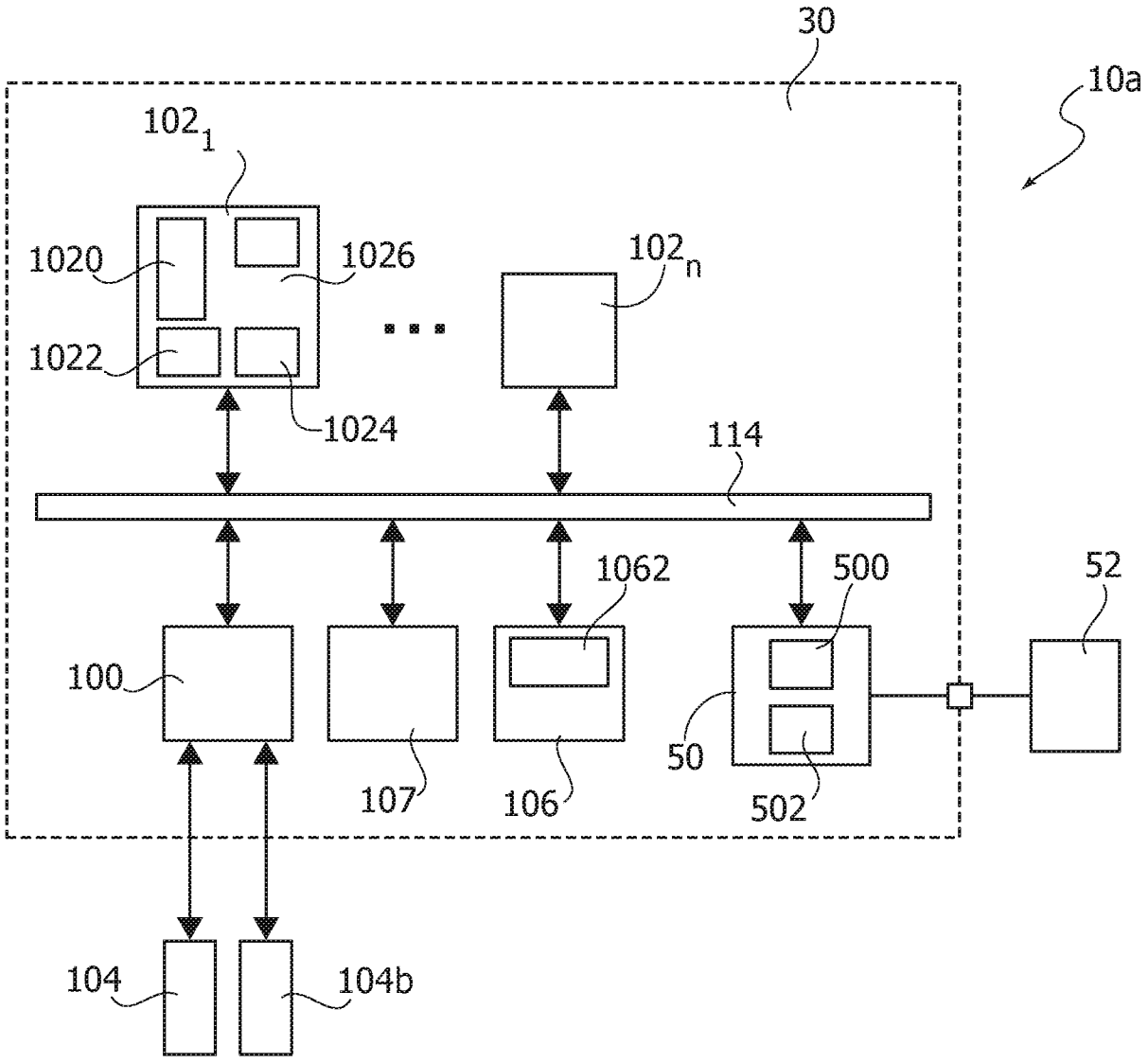

30
10a
102_1
1020
1026
102_n
1022
1024
114
1062
500
52
100
50
107
106
502
104
104b

FIG. 4

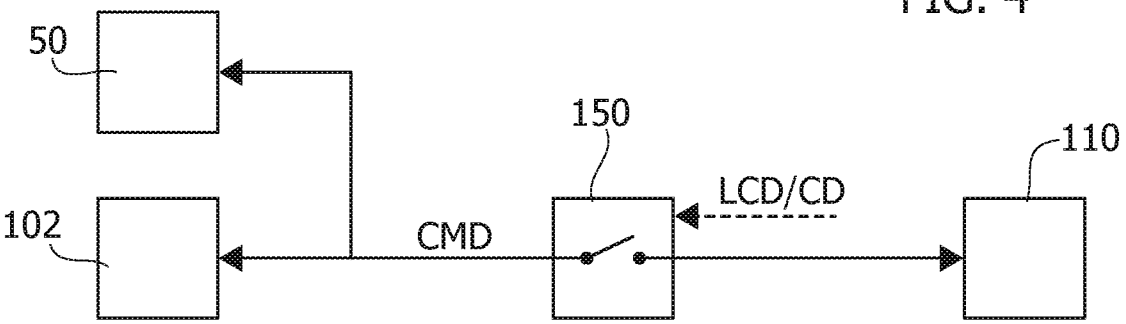


FIG. 5

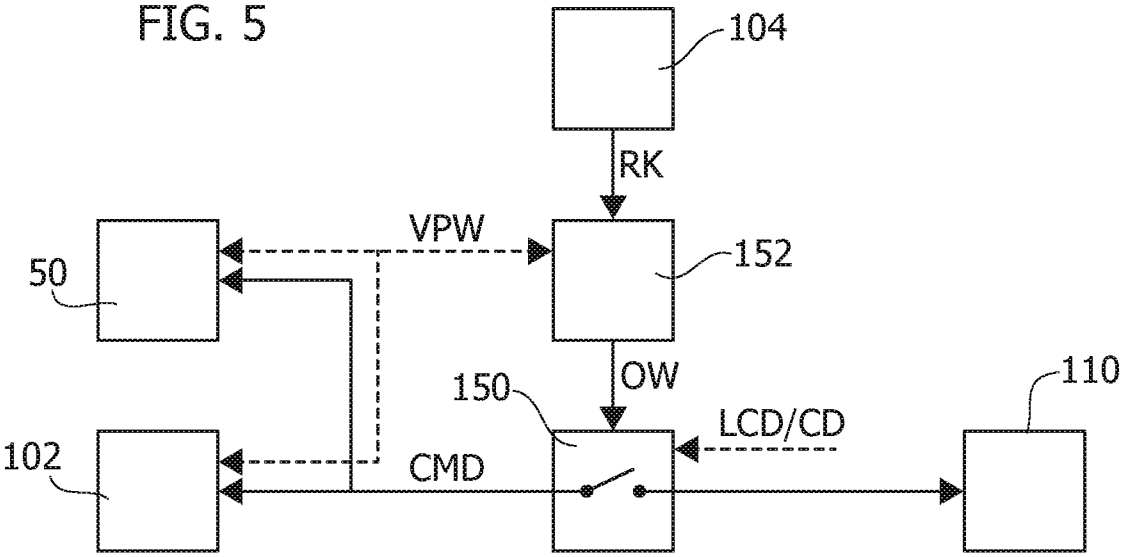


FIG. 6

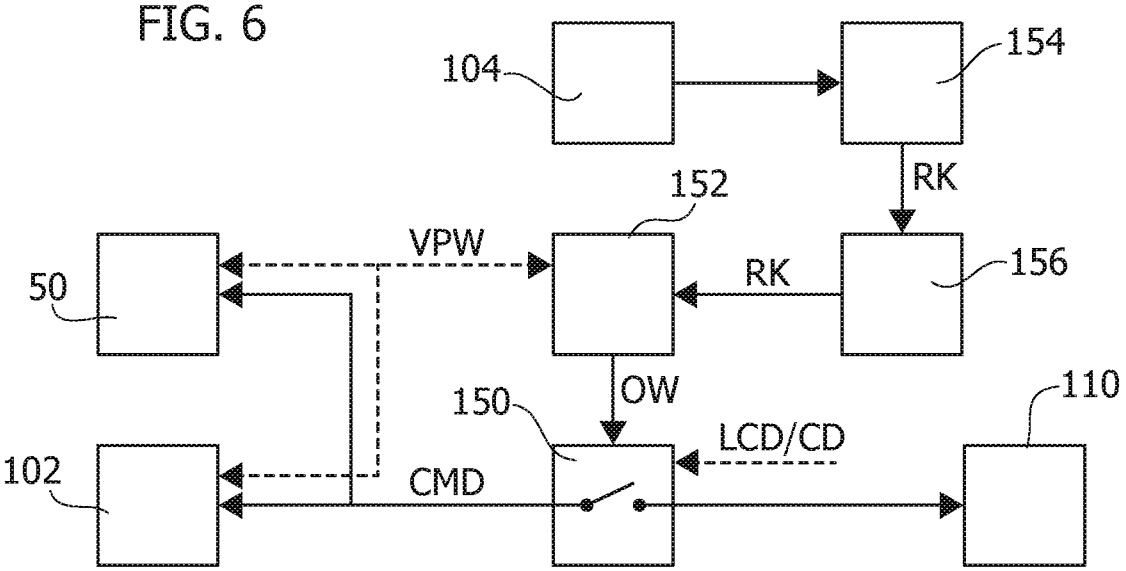


FIG. 7

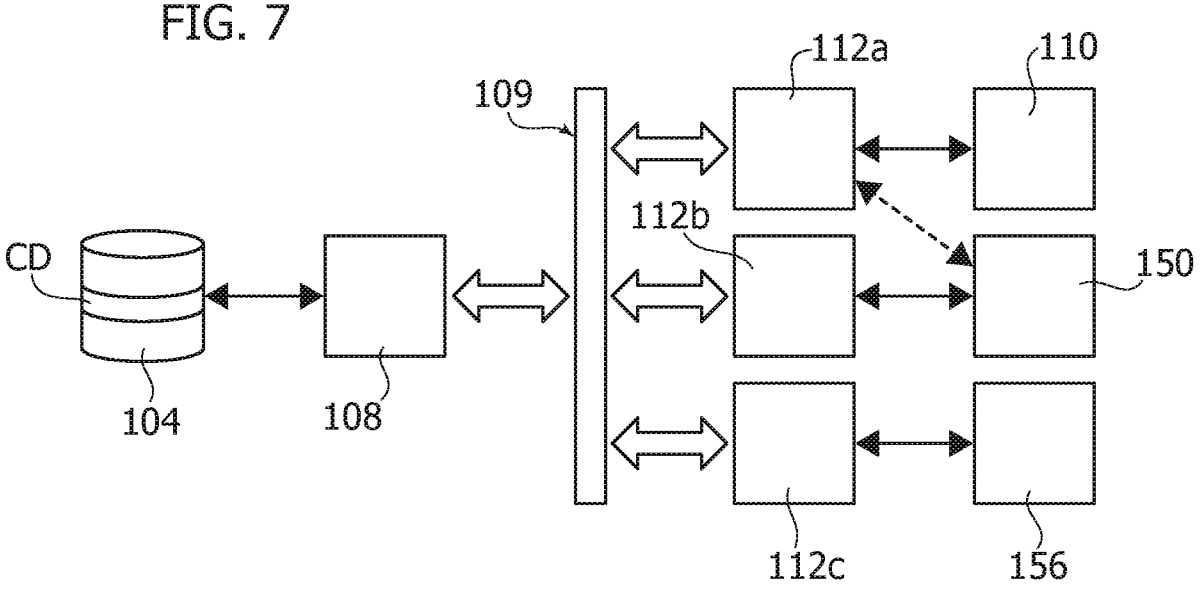

112a
110
109
112b
CD
150
104
108
112c
156

FIG. 8

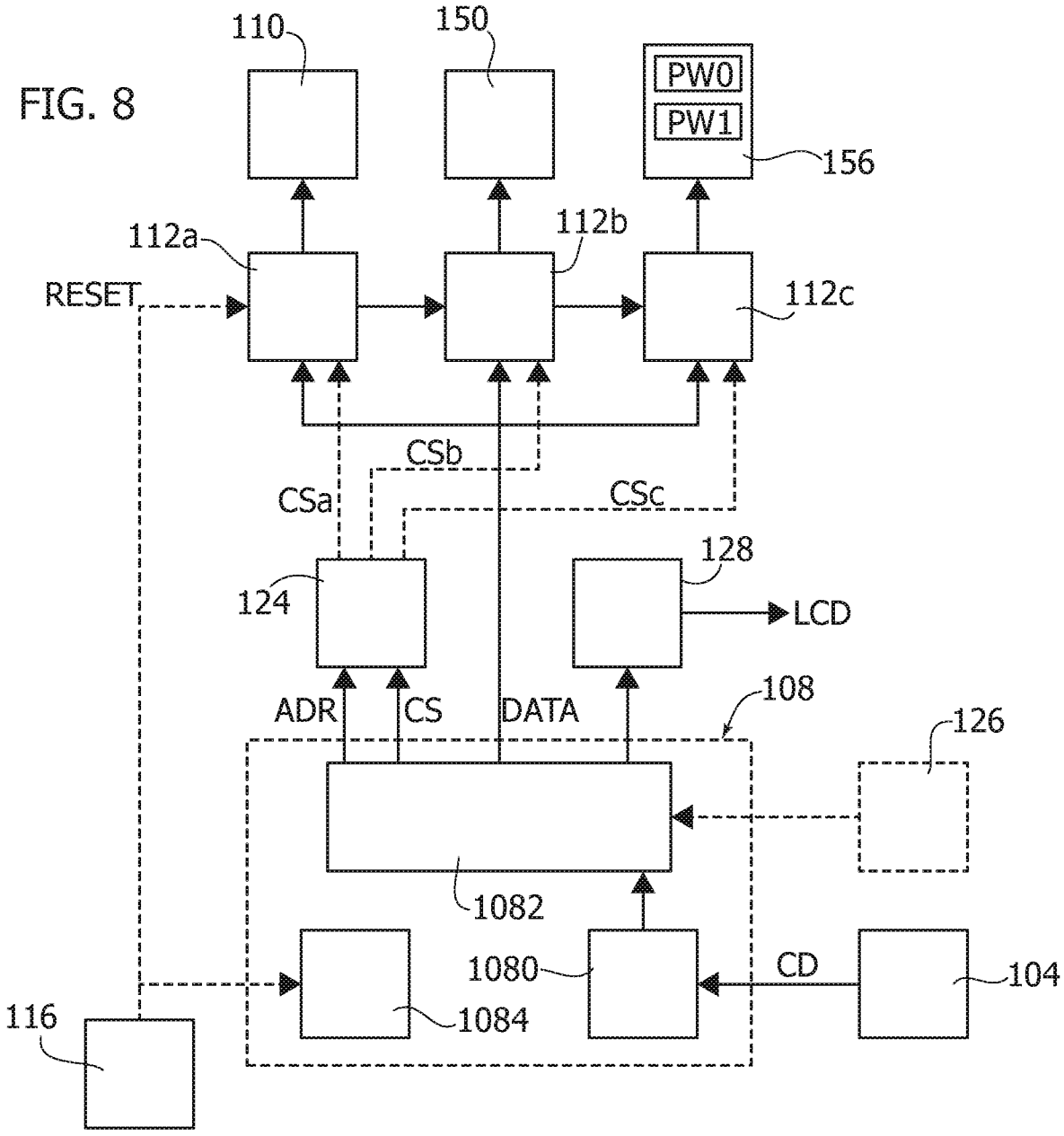

110
150
PW0
PW1
156
112a
112b
RESET
112c
CSb
CSa
CSc
128
124
LCD
ADR
CS
DATA
108
126
1082
1080
CD
104
1084
116

FIG. 9

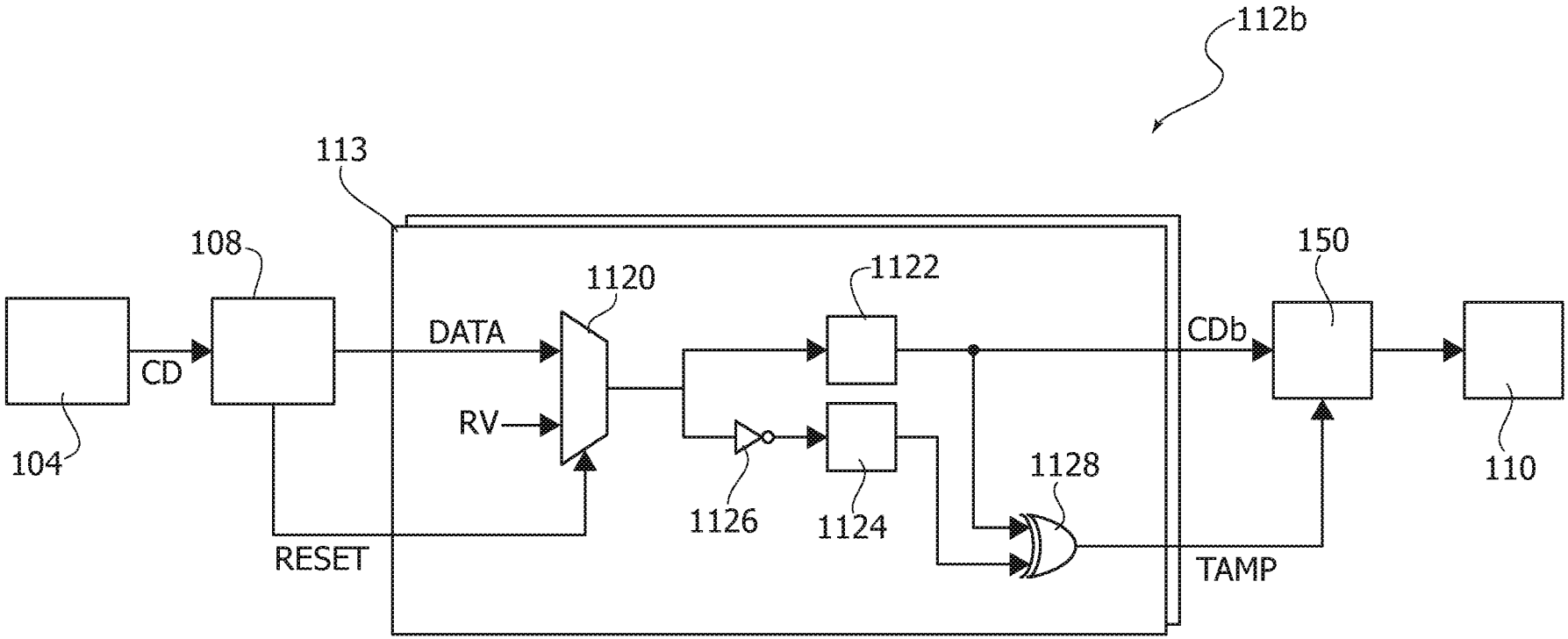

112b
113
108
150
1120
1122
DATA
CDb
CD
RV
104
110
1126
1124
1128
RESET
TAMP

FIG. 10

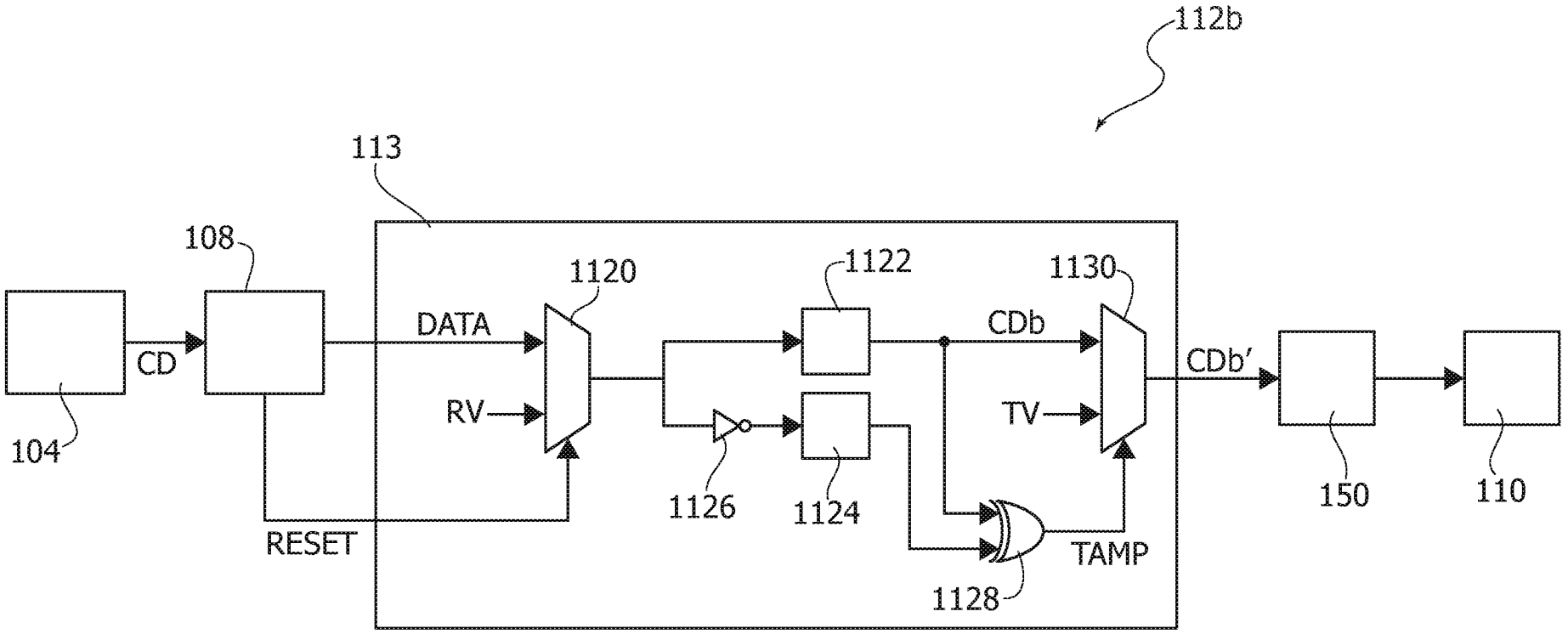

112b
113
108
1120
1122
1130
DATA
CDb
CD
RV
TV
CDb'
104
1126
1124
150
110
RESET
TAMP
1128

FIG. 11

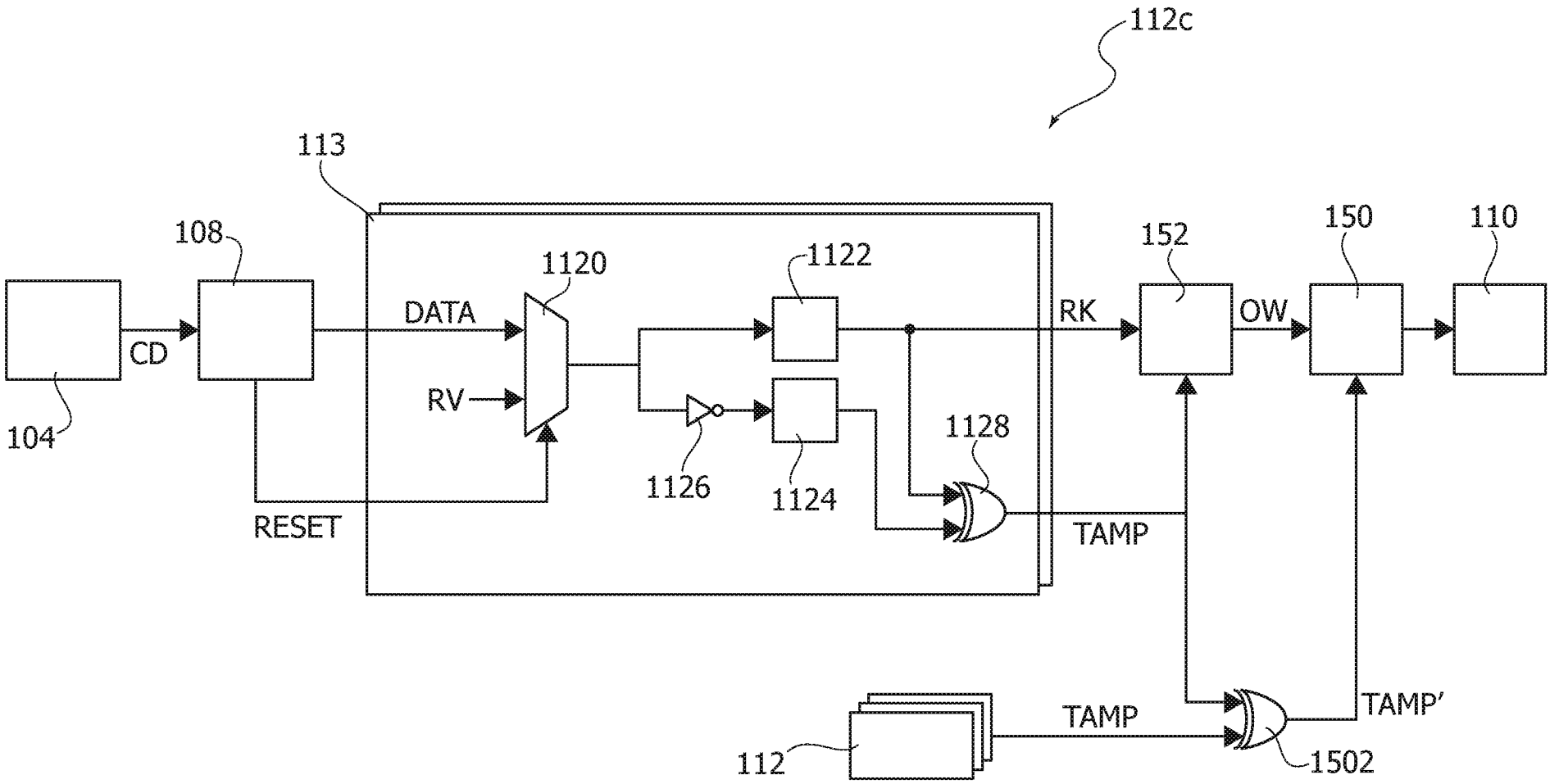
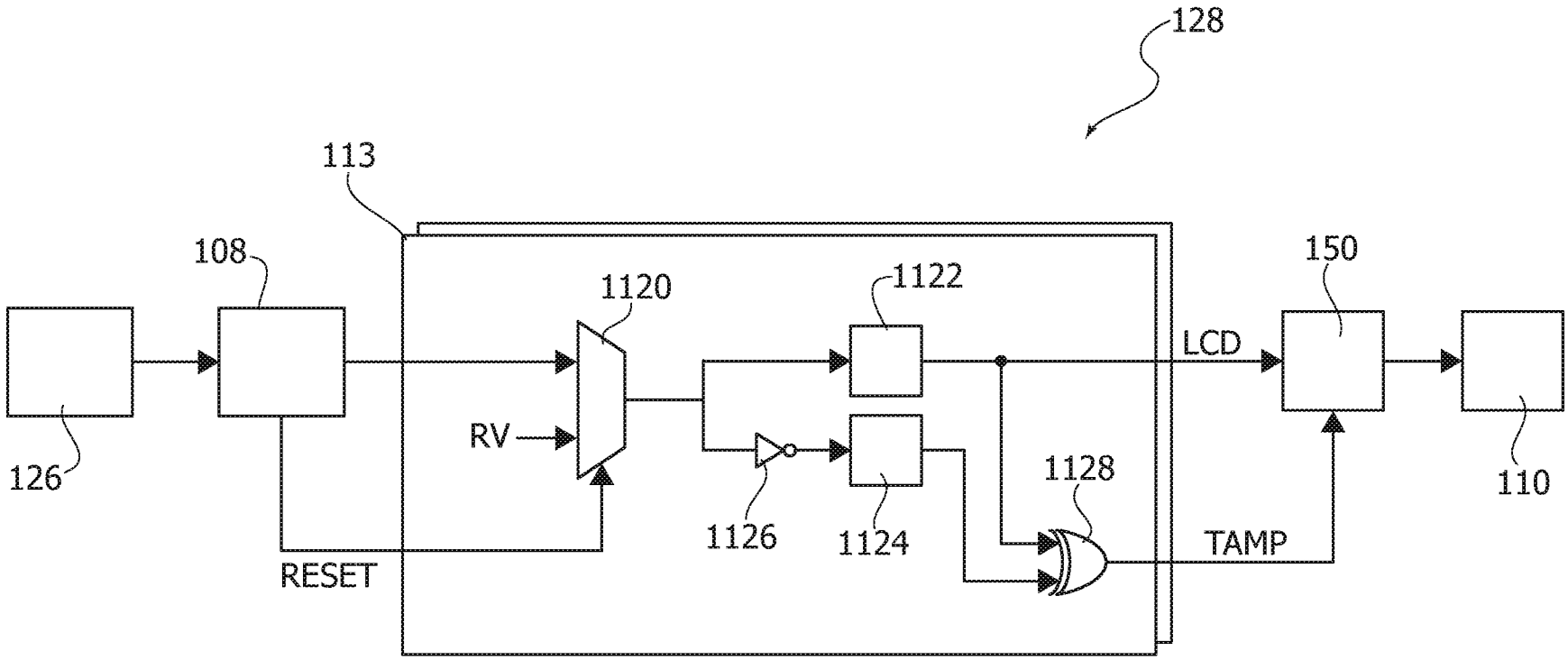

112c
113
108
104
CD
DATA
RV
1120
1122
1126
1124
1128
RESET
TAMP
RK
152
OW
150
110
112
TAMP
TAMP'
1502

FIG. 12


128
113
108
1120
1122
150
LCD
RV
126
1126
1124
1128
110
RESET
TAMP