(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6748117号
(P6748117)
(45)発行日　令和2年8月26日(2020.8.26)　(24)登録日　令和2年8月11日(2020.8.11)

(51)Int.Cl.　　F I
G11C 11/22 (2006.01)　　G11C 11/22 240
G06F 8/654 (2018.01)　　G11C 11/22 250
　　G06F 8/654

請求項の数 17　(全 22 頁)

(21)出願番号　特願2017-563054(P2017-563054)
(86)(22)出願日　平成28年6月2日(2016.6.2)
(65)公表番号　特表2018-526760(P2018-526760A)
(43)公表日　平成30年9月13日(2018.9.13)
(86)国際出願番号　PCT/US2016/035578
(87)国際公開番号　WO2016/196835
(87)国際公開日　平成28年12月8日(2016.12.8)
審査請求日　令和1年5月22日(2019.5.22)
(31)優先権主張番号　15/139,865
(32)優先日　平成28年4月27日(2016.4.27)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/169,930
(32)優先日　平成27年6月2日(2015.6.2)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　390020248
日本テキサス・インスツルメンツ合同会社
東京都新宿区西新宿六丁目２４番１号
(73)特許権者　507107291
テキサス　インスツルメンツ　インコーポレイテッド
アメリカ合衆国　テキサス州　７５２６５－５４７４　ダラス　メイル　ステイション　３９９９　ピーオーボックス　６５５４７４
(73)特許権者　512190309
テキサス　インスツルメンツ　ドイチュランド　ゲーエムベーハー
ドイツ連邦共和国　フライジング　８５３５６　ハッガーティシュトラーセ　１
最終頁に続く

(54)【発明の名称】ファームウェア更新のための強誘電メモリの拡張

(57)【特許請求の範囲】
【請求項１】
集積回路における強誘電体ランダムアクセスメモリ（ＦＲＡＭ）アレイにストアされる内容を更新する方法であって、前記ＦＲＡＭアレイが、行及び列に配されるメモリセルを含み、前記ＦＲＡＭアレイの各メモリセルが、通常動作モードにおいて２トランジスタ２コンデンサ（２Ｔ２Ｃ）メモリセルとして動作可能であり、更新モードにおいて第１及び第２の１トランジスタ１コンデンサ（１Ｔ１Ｃ）ハーフセルとして動作可能であり、前記方法が、
複数の前記メモリセルの各メモリセルにおいて相補分極状態として第１のデータセットをストアすることと、
前記ＦＲＡＭアレイを前記更新モードにすることと、
選択される複数の前記メモリセルの各メモリセルの前記第２のハーフセルにおいて第２のデータセットを書き込むことと、
前記第２のデータセットを検証することと、
前記第２のデータセットを成功裏に検証することに応答して、前記選択された複数のメモリセルの各メモリセルの前記第１のハーフセルに前記第２のデータセットの論理的相補を書き込むことと、
次いで、前記ＦＲＡＭアレイを前記通常動作モードにすることと、
を含む、方法。
【請求項２】

請求項１に記載の方法であって、
前記検証することが前記第２のデータセットにおける誤りを示すことに応答して、前記選択された複数のメモリセルの各メモリセルの前記第２のハーフセルに前記第１のデータセットを書き込むことを更に含む、方法。
【請求項３】
請求項２に記載の方法であって、
前記検証することが、
前記選択された複数のメモリセルの前記第２のハーフセルから前記第２のデータセットを読み出すことと、
読み出された前記第２のデータセットに対して数値的データ検証を実行することと、
を含む、方法。
【請求項４】
請求項２に記載の方法であって、
ネットワークリンクを介して更新ソースから前記第２のデータセットを受け取ることと、
前記検証することが前記第２のデータセットにおける誤りを示すことに応答して、前記更新ソースに失敗した検証を通知することと、
を更に含む、方法。
【請求項５】
請求項１に記載の方法であって、
前記通常動作モードにおいて、行アドレスに応答してメモリセルの行を選択することと、
前記選択された行における１つ又は複数のメモリセルの内容を感知することと、
を更に含む、方法。
【請求項６】
請求項５に記載の方法であって、
メモリセルの各行に対し、前記行の前記第１のハーフセルが第１の行アドレス値に関連付けられ、前記行の前記第２のハーフセルが前記第１の行アドレス値から単一行アドレスビットだけ異なる第２の行アドレス値に関連付けられ、
前記単一行アドレスビットが、前記通常動作モードにおける前記選択することにおいてマスクされる、方法。
【請求項７】
請求項６に記載の方法であって、
前記感知することが、前記選択された行の前記１つ又は複数のメモリセルの、それぞれ、前記第１及び第２のハーフセルに結合される第１のビットラインと第２のビットラインとの間の差動信号を感知することを含む、方法。
【請求項８】
請求項６に記載の方法であって、
前記検証することが、
前記選択された複数のメモリセルの前記第２のハーフセルから前記第２のデータセットを読み出すことと、
読み出された前記第２のデータセットに対して数値的データ検証を実行することと、
を含み、
前記読み出すことが、
前記単一行アドレスビットを含む行アドレスに対応するメモリセルの行において前記第２のハーフセルを選択することと、
前記選択された行における１つ又は複数のメモリセルの前記第２のハーフセルに結合される第２のビットラインにおける信号を基準電圧と比較することと、
を含む、方法。
【請求項９】

請求項５に記載の方法であって、
前記ＦＲＡＭメモリの内容が、実行可能プログラム命令に対応し、
前記方法が、前記１つ又は複数メモリセルの前記感知された内容に対応するプログラム命令を実行するためにプログラマブルロジックを動作させることを更に含む、方法。
【請求項１０】
集積回路であって、
実行可能なプログラムコードを格納し、通常動作モードにおいて２トランジスタ２コンデンサ（２Ｔ２Ｃ）メモリとしてのみ動作可能であり、更新モードにおいて１トランジスタ１コンデンサ（１Ｔ１Ｃ）メモリとしてのみ動作可能である強誘電体ランダムアクセスメモリ（ＦＲＡＭ）であって、
行及び列に配されるメモリセルのアレイであって、各列における前記メモリセルが第１及び第２のビットラインに結合され、前記アレイにおける各メモリセルが第１及び第２のハーフセルを含み、前記第１及び第２のハーフセルの各々が強誘電体コンデンサとパストランジスタとを含む、前記メモリセルのアレイと、
複数の感知アンプであって、各々が、メモリセルの列に関連付けられ、当該列に対する前記第１及び第２のビットラインに結合される、前記複数の感知アンプと、
を含む、前記ＦＲＡＭと、
一連の動作によって、前記実行可能なプログラムコードを更新するように前記ＦＲＡＭに結合される論理回路要素であって、前記一連の動作が、
複数の前記メモリセルの各メモリセルにおける相補分極状態として前記実行可能なプログラムコードを格納することと、
前記ＦＲＡＭを前記更新モードにすることと、
選択される複数の前記メモリセルの各メモリセルの前記第２のハーフセルに更新された実行可能なプログラムコードを書き込むことと、
前記更新された実行可能なプログラムコードを検証することと、
前記更新された実行可能なプログラムコードを成功裏に検証することに応答して、前記選択された複数のメモリセルの各メモリセルの前記第１のハーフセルに前記更新された実行可能なプログラムコードの論理的相補を書き込むことと、
次いで、前記ＦＲＡＭを前記通常動作モードにすることと、
を含む、前記論理回路要素と、
を含む、集積回路。
【請求項１１】
請求項１０に記載の集積回路であって、
前記ＦＲＡＭが、行アドレス値をデコードし、前記行アドレス値に応答してメモリセルの前記アレイの行のためのワードラインに通電するデコード回路要素を更に含み、
メモリセルの各行に対して、当該行における前記第１のハーフセルの各々の前記パストランジスタが、第１のワードライン信号に応答して、前記第１のハーフセルの強誘電体コンデンサのプレートを第１の行アドレス値に関連付けられて前記行における前記メモリセルの前記第１のハーフセル間で共有される前記第１のビットラインに結合し、
メモリセルの各行に対して、当該行における前記第２のハーフセルの各々の前記パストランジスタが、第２のワードライン信号に応答して、前記第２のハーフセルの強誘電体コンデンサのプレートを第２の行アドレス値に関連付けられて前記行における前記メモリセルの前記第２のハーフセル間で共有される前記第２のビットラインに結合し、
同じ行に対する前記第１及び第２の行アドレス値が、単一行アドレスビットだけ互いに異なる、集積回路。
【請求項１２】
請求項１１に記載の集積回路であって、
前記論理回路要素が、前記通常動作モードにおいて、一連の動作によって１つ又は複数のメモリセルの内容を読み出すよう前記ＦＲＡＭを制御し、前記一連の動作が、
前記デコード回路要素に行アドレスを印加することと、

前記単一行アドレスビットをマスクしながら、前記行アドレスに対応するメモリセルの前記アレイの行を選択するように前記デコード回路要素を制御することと、
前記第１のビットラインと前記第２のビットラインとの間の差動信号を感知するように前記複数の感知アンプの１つ又は複数を動作させること、
を含み、
前記更新モードにおいて、前記検証することが、
前記デコード回路要素に行アドレスを印加することと、
前記単一行アドレスビットを含む前記行アドレスに対応するメモリセルの前記アレイの行を選択するように前記デコード回路要素を制御することと、
前記第２ビットラインにおける信号を基準電圧と比較するように前記複数の感知アンプの１つ又は複数を動作させることと、
によって、前記選択された複数のメモリセルの前記第２のハーフセルから前記更新された実行可能なプログラムコードを読み出すことを含む、集積回路。
【請求項１３】
請求項１２に記載の集積回路であって、
前記ＦＲＡＭが、前記単一行アドレスビットに応答して、前記更新モードにおいて前記列の各列の前記第１及び第２のビットラインの一方に基準電圧を結合する回路要素を更に含む、集積回路。
【請求項１４】
請求項１０に記載の方法であって、
前記ＦＲＡＭに格納され、前記ＦＲＡＭから引き出されるプログラム命令を実行するプログラマブル論理を更に含み、
前記論理回路要素が、前記ＦＲＡＭの内容を更新するように前記ＦＲＡＭを制御し、前記通常動作モードにおいて、前記ＦＲＡＭにデータを格納し、前記ＦＲＡＭからデータを引き出すメモリコントローラ論理を含む、集積回路。
【請求項１５】
請求項１０に記載の集積回路であって、
前記一連の動作が、前記検証することが前記更新された実行可能なプログラムコードにおける誤りを示すことに応答して、前記選択された複数のメモリセルの各メモリセルの前記第２のハーフセルに前記実行可能なプログラムコードを書き込むことを更に含む、集積回路。
【請求項１６】
請求項１５に記載の集積回路であって、
前記検証することが、
前記選択された複数のメモリセルの前記第２のハーフセルから前記更新された実行可能なプログラムコードを読み出すことと、
読み出された前記更新された実高可能なプログラムコードに対して数値的データ検証を実行することと、
を含む、集積回路。
【請求項１７】
集積回路であって、
実行可能なプログラムコードを格納する不揮発性メモリであって、
行及び列に配されるメモリセルのアレイであって、各メモリセルが、各々が不揮発性メモリ要素を含む第１及び第２のハーフセルを含み、前記第１のハーフセルが、アクセスされるとき第１のビットラインに結合され、前記第２のハーフセルが、アクセスされるとき第２のビットラインに結合され、前記第１及び第２のビットラインが、前記アレイの同じ列のメモリセルにより共有される、前記メモリセルのアレイと、
複数の感知アンプであって、各々が、メモリセルの列に関連付られ、当該列のための前記第１及び第２のビットラインに結合される、前記複数の感知アンプと、
を含む、前記不揮発性メモリと、

一連の動作によって前記実行可能なプログラムコードを更新するように前記メモリに結合される論理回路要素であって、前記一連の動作が、
複数の前記メモリセルの各メモリセルにおける相補データ状態として前記実行可能なプログラムコードを格納することと、
前記メモリを単に更新モードにすることであって、前記更新モードにおいて各メモリセルの前記第１及び第２のハーフセルが別々にアクセスされる、前記更新モードにすることと、
選択される複数の前記メモリセルの各メモリセルの前記第２のハーフセルに更新された実行可能なプログラムコードを書き込むことと、
前記更新された実行可能なプログラムコードを検証することと、
前記更新された実行可能なプログラムコードを成功裏に検証することに応答して、前記選択された複数のメモリセルの各メモリセルの前記第１のハーフセルに前記更新された実行可能なプログラムコードの論理的相補を書き込むことと、
前記メモリを単に通常動作モードにすることであって、前記通常動作モードにおいて、アクセスされるメモリセルの前記第１及び第２のハーフセルが、対応する列に対して、それぞれ、前記第１及び第２のビットラインに結合される、前記通常動作モードにすることと、
を含む、前記論理回路要素と、
を含む、集積回路。

【発明の詳細な説明】

【技術分野】

【０００１】

本願は、概して、埋込み強誘電メモリリソースを組み込む電子システムに関し、より特定していえば、これらの埋込みメモリリソースの内容を更新するためのシステム及びこういったシステムを動作させる方法に関する。

【背景技術】

【０００２】

従来の金属酸化物半導体（ＭＯＳ）及び相補型ＭＯＳ（ＣＭＯＳ）論理及びメモリデバイスは、現代の電子システムにおいて普及している。これは、これらのデバイスが、それらの高密度、及び大規模集積に対する適合性とともに、高速スイッチング時間と低電力消費の優れた組合せを提供するからである。しかし、これらのデバイスは、これらの技術に従って構築される論理及びメモリ回路がバイアス電力を喪失するとそれらのデータ状態を保持しないという点で、本質的に揮発性である。特に携帯及び小型システムにおいて、メモリ及び論理状態を不揮発的にストアする能力が望ましい。その結果、最近、不揮発デバイスを構築するための様々な技術が開発されてきている。

【０００３】

不揮発ソリッドステートメモリデバイスを実現するために近年開発された或る技術は、誘電材料が、非強誘電コンデンサで典型的に使用される二酸化シリコン又はシリコン窒化物ではなく、ジルコン酸チタン酸鉛（ＰＺＴ）又はタンタル酸ストロンチウムビスマス（ＳＢＴ）などの分極可能な強誘電材料であるコンデンサの構造に関与する。強誘電材料の分極状態に基づく電荷－電圧（Ｑ－Ｖ）特性におけるヒステリシスにより、これらのコンデンサにおいて２値状態の不揮発性ストアが可能になる。これに対して、従来のＭＯＳコンデンサでは、それらのストアされた電荷がデバイスの電源オフ時に失われる。強誘電コンデンサは、現代のＣＭＯＳ集積回路と概ね互換性があるプロセスによって、例えば、金属導体の重なるレベルの間にトランジスタレベルよりも上でコンデンサを置くことによって、構築され得ることがわかっている。

【０００４】

図１は、従来の強誘電コンデンサのＱ－Ｖ特性の例を示す。図に示すように、導体プレートの両端間にストアされる電荷（Ｑ）は、これらのプレートに印加される電圧（Ｖ）に依存し、この電圧の最近の履歴にも依存する。コンデンサプレート両端間に印加される電

圧Ｖが「抗」電圧＋$Ｖ_{\alpha}$を超えると、コンデンサは「＋１」状態に分極する。この特性に従って、「＋１」状態に分極した後、電圧Ｖが抗電圧－$Ｖ_{\beta}$より大きいままである限り、コンデンサはストア電荷＋$Ｑ_{1}$を示す。逆に、コンデンサプレート両端間に印加される電圧Ｖが抗電圧－$Ｖ_{\beta}$より負になると、コンデンサは、「－１」状態に分極され、＋$Ｖ_{\alpha}$未満の印加電圧Ｖに対してストア電荷－$Ｑ_{2}$を示す。

【０００５】

集積回路における不揮発性ストアのための強誘電コンデンサの重要な特性の一つは、強誘電コンデンサが示す、その分極状態間の静電容量の差である。或る要素の静電容量を、印加電圧に対するストア電荷の比と称する。強誘電コンデンサの文脈において、分極電圧の印加の際に起こる分極状態の変化は、電荷ストアに反映される。例えば、図１を参照すると、強誘電コンデンサの「－１」状態から「＋１」状態への分極は、比較的大きな静電容量Ｃ（－１）において反映され、それによって、分極状態の変化に関わる分極電荷は、電圧が抗電圧$Ｖ_{\alpha}$を超えるとコンデンサ内に保持される。比較として、既に「＋１」状態にあるコンデンサは、分極のため極めて小さな静電容量Ｃ（＋１）を示す。これは、コンデンサの強誘電ドメインが電圧印加前に既に揃っているからである。いずれの場合でも、強誘電コンデンサも、それが誘電体膜（すなわち強誘電材料）によって離された平行プレートとして構築されているために、線形な静電容量を有する。下記の説明から明らかなように、ストア論理状態は、強誘電コンデンサの静電容量を問い合わしてその分極状態を識別することによって読み出される。

【０００６】

現在、強誘電技術は不揮発性ソリッドステート読出し／書込みランダムアクセスメモリ（ＲＡＭ）を実現するために用いられている。これらのメモリリソースは、一般に「強誘電ＲＡＭ」或いは「ＦｅＲＡＭ」又は「ＦＲＡＭ」と称し、いまや多くの電子システム、特に携帯電子デバイス及びシステムにおいて、ごく普通に用いられている。ＦＲＡＭは、ＦＲＡＭメモリが極低電力消費であるため、ペースメーカ、除細動器、及びモニタリングデバイスなどの移植可能な医療デバイスに特に魅力的である。

【０００７】

ＦＲＡＭの実装に対する１つの手法は、２トランジスタ・２コンデンサ（２Ｔ２Ｃ）強誘電メモリセルであり、この場合、セル内のこれら２つの強誘電コンデンサが相補的な状態に分極される。図２ａは、従来の２Ｔ２Ｃ構造のメモリセル$２_{j,k}$を概略的に図示する。この例において、セル$２_{j,k}$は、メモリアレイの行ｊ及び列ｋに存し、２つの強誘電コンデンサ４ａ、４ｂ及び２つの金属酸化物半導体（ＭＯＳ）トランジスタ５ａ、５ｂを含む。強誘電コンデンサ４ａ、４ｂは、誘電体としてＰＺＴなどの強誘電材料を用いる平行プレートコンデンサであり、これらのプレートの一方又は両方が、半導体材料（例えば、基板における拡散された領域、ポリシリコン）で或いは金属又は導電性金属化合物材料（例えば、シリサイド又は導電性窒化物）で形成され得る。各強誘電コンデンサ４ａ、４ｂの一方のプレートは、行ｊに対しプレートライン$ＰＬ_{j}$に接続される。強誘電コンデンサ４ａの他方のプレートは、ｐチャネルトランジスタ５ａのソース／ドレイン経路を介して列ｋに対しビットライン$ＢＬＴ_{k}$に接続され、同様に、強誘電コンデンサ４ｂの第２のプレートは、ｎチャネルトランジスタ５ｂのソース／ドレイン経路を介してビットライン$ＢＬＣ_{k}$に接続される。トランジスタ５ａ、５ｂのゲートは、メモリアレイの行ｊに対しワードライン$ＷＬ_{j}$によって駆動される。

【０００８】

動作において、強誘電コンデンサ４ａ、４ｂは、ビットライン$ＢＬＴ_{k}$、$ＢＬＣ_{k}$間の差動電圧又は電流として反映される相補分極状態を、読み込まれる際にストアする。したがって、従来のメモリセル$２_{j,k}$への書込み動作において、所望のデータ状態に対応する極性で相補レベルがビットライン$ＢＬＴ_{k}$、$ＢＬＣ_{k}$に印加され、ワードライン$ＷＬ_{j}$はアクティブハイに駆動されてトランジスタ５ａ、５ｂをオンにし、この状態の間のプレートライン$ＰＬ_{j}$におけるパルスにより、互いに逆の分極電圧がこれらに対応する相補分極状態にコンデンサ４ａ、４ｂを分極する。読出し動作において、ビットライン$ＢＬＴ_{k}$

、BLC_kが選択電圧にプリチャージされ、次いで、浮遊し、その後、ワードラインWL_jがアクティブハイにアサートされる。プレートラインPL_jにおけるパルスにより、コンデンサ４ａ、４ｂの相補分極状態が、それぞれ、ビットラインBLT_k、BLC_k間の差動信号として反映されて、列ｋに対し感知アンプ6_kによって感知及び増幅される。

【０００９】

図２ｂは、図２ａに従って構築されるものなど、メモリセル２の従来のメモリアレイ５の簡略化された配置をブロック形式で図示する。実際の集積回路におけるメモリアレイは図２ａに示すものよりもかなり大規模であり、そのため、この小型（４×４）の例は単に説明のために提供されている。図２ａのアレイ５において、アレイ内のセル２の各行は、ワードラインWL_0～WL_3のうちの対応するワードライン、及びプレートラインPL_0～PL_3の１つに関連付られている。セル２の各列は１対のビットラインを共有し、列０がビットラインBLT_0、BLC_0に結合され、列１がビットラインBLT_1、BLC_1に結合され、以下同様である。感知アンプ6_0がビットラインBLT_0、BLC_0を受け、感知アンプ6_1がビットラインBLT_1、BLC_1を受け、感知アンプ6_2がビットラインBLT_2、BLC_2を受け、感知アンプ6_3がビットラインBLT_3、BLC_3を受ける。したがって、セル２の行ｊに対するワードラインWL_j及びプレートラインPL_jに通電することにより、（場合に応じて）セル$2_{j,0}$～$2_{j,3}$からのデータの読み出し又はセル$2_{j,0}$～$2_{j,3}$へのデータの書き込みが、それぞれ、ビットライン対BLT_0、BLC_0～BLT_3、BLC_3を介して成される。

【００１０】

図２ａ及び図２ｂの従来の２Ｔ２Ｃ配置は、差動感知配置による確実な読出しマージンが得られるため、良好な長期データ保持を提供することが確認されている。所与のセル$2_{j,k}$における誘電コンデンサ４ａ、４ｂの一方が製造時に脆弱でも、又は、デバイスの動作寿命の間に分極が大きく喪失しても、対向コンデンサがより強い分極状態を保持する限り、このセルは依然として正しいデータ状態を戻し得る。

【００１１】

これに対し、従来のダイナミックＲＡＭメモリセルに類似する１Ｔ１Ｃ（１トランジスタ、１コンデンサ）配置で構築される強誘電セルは、その小さなチップ面積のために魅力的である。図２ｃは、類似セル１２のアレイの行ｊ及び列ｋに存在する単一セルを表す従来の１Ｔ－１Ｃ　ＦＲＡＭセル12_{jk}の例示配置を示す。セル12_{jk}は、強誘電コンデンサ１４及びｎチャネルパストランジスタ１５を含む。トランジスタ１５のソース／ドレイン経路は、アレイの列ｋに対するビットラインBL_kと、強誘電コンデンサ１４の頂部プレートとの間に接続され、トランジスタ１５のゲートは、アレイの行ｊに対してワードラインWL_jによって制御される。強誘電コンデンサ１４の底部プレートは、この行のプレートラインＰＬに接続されるか、又は、アーキテクチャによっては、この底部プレートは、アレイにおける又はアレイ部分におけるすべてのセル１２について共通であり得る。したがって、１Ｔ－１ＣＦＲＡＭセルは、従来のダイナミックＲＡＭメモリセルと同様に構築される。感知アンプ16_kは、ビットラインBL_kに結合され、読出し電流i_Rによってつくられるビットライン電圧を、基準電圧生成器によって生成されるか又は基準コンデンサによって生成され得る「ダミー」ビットラインにおける基準電圧V_{REF}と比較するように動作する。この基準電圧V_{REF}は、通常、「０」及び「１」データ状態に対する予期電圧間の中間レベルである。

【００１２】

１Ｔ１Ｃ及び２Ｔ２Ｃ　ＦＲＡＭセルアーキテクチャを比較すると、１Ｔ１Ｃセルは、ビット密度が高いという利点を有するが、読出しマージンが小さいという欠点を有する。これは、１Ｔ１Ｃが基準電圧に対してシングルエンド感知を行うためであり、一方、２Ｔ２Ｃセルは、相補データストア及び差動感知によりデータ保持が確実という利点を有するが、ビット密度は約半分に過ぎない。

【００１３】

上述したように、ＦＲＡＭ不揮発性メモリは、多くの電子システムにおいて用いられる

ことが一般的になっている。テキサス・インスツルメンツ・インコーポレーテッドから入手可能なマイクロコントローラのＭＳＰ４３０ファミリーなどのいわゆる「システムオンチップ」（ＳｏＣ）デバイスは、いまではＦＲＡＭリソースを含むことが多い。離れた場所に配置され、そのため電力消費が特に問題となる、センサ及びコントローラを実現するために用いられる場合に特にそうである。Ｚｗｅｇらの「An 82 mA/MHz Microcontroller with Embedded FeRAM for Energy-Harvesting Applications」、Digest of Technical Papers、2011 Int 'l Solid-State Circ. Conf、 論文１９．２（ＩＥＥＥ）、頁３３４～３６は、このようなマイクロコントローラベースのＳｏＣの例を記載しており、この文献は、参照により本明細書に組み込まれる。いわゆる「モノのインターネット」（ＩｏＴ）に従ったこれら及び類似のＳｏＣデバイスのネットワーキングが普及しつつある。

【非特許文献１】Zwerg et al., "An 82 mA/MHz Microcontroller with Embedded FeRAM for Energy-Harvesting Applications", Digest of Technical Papers, 2011 Int'l Solid-State Circ. Conf, paper 19.2 (IEEE), pp. 334 - 36

【００１４】

特にこれらのネットワーク化された実装形態において、特定のセンサ又はコントローラが所望の機能を行なう拠り所となる実行可能プログラムコードを含めて、マイクロコントローラの「ファームウェア」をストアするためにＦＲＡＭが用いられることが多い。これらの遠隔配置ＩｏＴデバイスの予期システム寿命を考慮して、ＳｏＣアーキテクチャは、典型的に、新たに受信した更新されたファームウェアをそれをインストールする前に検証して更新後の操作性を保証する能力を含めて、システムファームウェアを更新するための何らかの備えを含む。従来のアーキテクチャにおいて、ＦＲＡＭ内の既存のファームウェア像に上書きする前に、この確認の間、更新されたファームウェアをストアするためにメモリスペースにおけるバッファが必要である。このバッファは、ＳｏＣデバイス内の付加的なメモリを必要とし、そのため、デバイスのチップ面積及び製造コストが増大し、潜在的にＳｏＣの電力消費に影響を及ぼす。いくつかのシステムアーキテクチャにおいて、付加的なメモリデバイス（例えばＲＡＭ）が、検証前の更新されたファームウェアをストアするためのバッファとして、ＳｏＣデバイスの外部に提供される。付加的なバッファをＳｏＣデバイス内に実装するコストは避けられるが、この外部バッファは、システム全体のコスト及び複雑さを増大させる。

【００１５】

さらなる背景として、メモリセルが２Ｔ２Ｃ又は１Ｔ１Ｃモードのいずれかで選択的に動作され得る従来のＦＲＡＭアーキテクチャがある。このようなアーキテクチャの例が米国特許番号第５，７５１，６２８号に説明されており、これは、参照により本明細書に組み込まれている。特許番号第５，７５１，６２８号の例では、制御信号が、付加的な行アドレスラインがデコードされるべきか否かを選択し、この場合、ＦＲＡＭセルが１Ｔ１Ｃセルとして動作される（すなわち、書込み及び読出しが行われる）。１Ｔ１Ｃモードにおける読出しサイクルでは、ダミーワードラインがアクティブにされて、基準メモリセルコンデンサを、アドレスされた１Ｔ１Ｃセルが結合されるビットラインの反対のビットラインに結合する。次いで、感知アンプが、アドレスされた１Ｔ１Ｃセルのデータ状態を、基準メモリセルコンデンサによって生成されるビットライン電圧との比較によって感知する。逆に、２Ｔ２Ｃモードにおける読出しサイクルでは、ダミーワードラインがアクティブにされず、代わりに、２本のワードラインがアクティブにされて、隣接する行の同じ列のセルを対向ビットラインに結合し、感知アンプが差動感知を行う。

【特許文献１】米国特許番号第５，７５１，６２８号

【発明の概要】

【００１６】

説明される例において、大規模集積回路が、付加的なバッファを必要とすることなく更新され得るファームウェアを備えるプログラマブルロジックを含む。このような集積回路のファームウェアを更新する方法において、この方法は、更新された内容を検証前にストアするための付加的なバッファの使用を必要とすることなく実施される。このような回路

及び方法は、不揮発性読出し／書込みメモリを用いてファームウェアをこのように更新する能力を提供する。

【００１７】

説明される例において、集積回路が、プログラマブルロジックのための実行可能なコードをストアするための強誘電ランダムアクセスメモリ（ＦＲＡＭ）リソースを含み、論理回路要素及び対応する方法によってＦＲＡＭの内容が更新される。ＦＲＡＭは、通常動作モードにおいて２Ｔ２Ｃ　ＦＲＡＭメモリとして、及び、更新モードにおいて１ＴＣ１ＦＲＡＭメモリとして、選択的に動作するように構築される。ＦＲＡＭの内容を更新するために、ＦＲＡＭの動作モードが、メモリコントローラロジックによって更新（１ＴＣ１）モードに変更され、更新されたコードが、複数のメモリロケーションの各々において１ＴＣ１ハーフセルの一方に書き込まれ、オリジナルデータは、複数のメモリロケーションの各々において他方の１ＴＣ１ハーフセルにストアされる。更新された内容の検証に続いて、相補ハーフセルのオリジナルデータは、検証された更新されたデータで上書きされ、動作モードは、通常（２Ｔ２Ｃ）動作モードに戻される。

【図面の簡単な説明】

【００１８】

【図１】従来の強誘電コンデンサの電荷対電圧特性のグラフである。

【００１９】

【図２ａ】従来の２Ｔ２Ｃ強誘電メモリセル及びその動作を図示する概略ブロック形式の電気図である。

【００２０】

【図２ｂ】従来の強誘電ランダムアクセスメモリ（ＦＲＡＭ）アレイのアーキテクチャのブロック形式の電気図である。

【００２１】

【図２ｃ】従来の１Ｔ１Ｃ強誘電メモリセル及びその動作を図示する概略ブロック形式の電気図である。

【００２２】

【図３】実施形態に従って構成されるＳｏＣデバイスのアーキテクチャのブロック形式の電気図である。

【００２３】

【図４】実施形態に従って構成される、図３のＳｏＣデバイスにおけるＦＲＡＭサブシステムのアーキテクチャのブロック形式の電気図である。

【００２４】

【図５】或る実施形態に従った、図３のアーキテクチャにおけるＦＲＡＭアレイの一部の配置を図示する概略ブロック形式の電気図である。

【００２５】

【図６】或る実施形態に従ったＦＲＡＭアレイの内容を更新する動作を図示するフローチャートである。

【００２６】

【図７ａ】この実施形態に従った図６のプロセスの間の様々な段階での図３のアーキテクチャにおけるＦＲＡＭアレイの内容を図示するブロック図である。

【図７ｂ】この実施形態に従った図６のプロセスの間の様々な段階での図３のアーキテクチャにおけるＦＲＡＭアレイの内容を図示するブロック図である。

【図７ｃ】この実施形態に従った図６のプロセスの間の様々な段階での図３のアーキテクチャにおけるＦＲＡＭアレイの内容を図示するブロック図である。

【図７ｄ】この実施形態に従った図６のプロセスの間の様々な段階での図３のアーキテクチャにおけるＦＲＡＭアレイの内容を図示するブロック図である。

【図７ｅ】この実施形態に従った図６のプロセスの間の様々な段階での図３のアーキテクチャにおけるＦＲＡＭアレイの内容を図示するブロック図である。

【図７ｆ】この実施形態に従った図６のプロセスの間の様々な段階での図３のアーキテク

チャにおけるＦＲＡＭアレイの内容を図示するブロック図である。

【発明を実施するための形態】

【００２７】

例示の実施形態は、いわゆる「システムオンチップ」又は「ＳｏＣ」などの大規模集積回路に実装され得る。また、例示の実施形態は、他の応用例において及び他の使用のために有益に実施され得る。

【００２８】

図３は、これらの実施形態に従って構築されるＳｏＣ４００の一般化されたアーキテクチャをブロック図形式で図示する。この例において、ＳｏＣ４００の中央処理装置（ＣＰＵ）として働くプログラマブルロジックがＣＰＵ４３０によって提供される。ＣＰＵ４３０は、ＡＲＭプロセッサ、又はテキサス・インスツルメンツ・インコーポレーテッドから入手可能なＭＳＰ４３０ファミリーのマイクロコントローラにおいて用いられる１６ビットＲＩＳＣプロセッサコアなどの、マイクロプロセッサとし得る。ＳｏＣ４００は複数のＣＰＵ４３０を含むように構築され得る。複数のＣＰＵ４３０は、ＳｏＣ４００の特定の機能に対して適切なように、互いに同じタイプとすることもできるし、汎用プログラマブルプロセッサ、デジタルシグナルプロセッサ（ＤＳＰ）、又は固定シーケンス生成器を含めて他の特定用途向け又はカスタム論理などの他のタイプのプロセッサとすることもできる。図３に示すように、ＣＰＵ４３０は、制御レジスタ４３１を含めて１つ又は複数のレジスタバンクを含み得る。

【００２９】

ＳｏＣ４００におけるメモリリソースは、強誘電ランダムアクセスメモリ（ＦＲＡＭ）４１０、読出し専用メモリ（ＲＯＭ）４３２、及びランダムアクセスメモリ４１２によって提供され、これら各メモリの一部には、ＣＰＵ４３０がメインアドレスバスＭＡＢ及びメインデータバスＭＤＢを介してアクセス可能である。ＦＲＡＭ４１０、ＲＯＭ４３２、及びＲＡＭ４１２は、図３において単体ブロックとして示されているが、これらのメモリリソースは、代替として複数メモリブロック又はアレイとして実現され得る。例えば、ＲＡＭ４１２は、スタティックＲＡＭ（ＳＲＡＭ）及びダイナミックＲＡＭ（ＤＲＡＭ）など、多くのメモリセルタイプ及び配置の任意の１つ又は複数として実現され得る。この実施形態におけるＦＲＡＭ４１０は、ＦＲＡＭコントローラロジック４１１を介してバスＭＡＢ、ＭＤＢに結合され、ＦＲＡＭコントローラロジック４１１の機能及び動作は、ＦＲＡＭ４１０の内容の更新に関連して下記で詳細に説明する。ＦＲＡＭ４１０は、不揮発性であり低電力消費なので、ＳｏＣ４００の「ファームウェア」をストアするのによく適している。このようなファームウェアは、その通常動作においてＳｏＣ４００によって成される１つ又は複数のアプリケーションのための実行可能プログラムコードを構成する。このファームウェアは、これらの実施形態の動作を説明する本明細書で説明する例において更新され得る。このアーキテクチャにおけるＲＯＭ４３２は、「ブートローダ」メモリ（「ＢＳＬ」）として働き、ＣＰＵ４３０によって実行され得るプログラムコードをそのようにストアする。

【００３０】

アドレスバスＭＡＢ及びデータバスＭＤＢを介してアクセス可能な様々なメモリリソース４１０、４１２、４３０に加えて、ＳｏＣ４００内の回路機能の多くが、それら自体で、ＣＰＵ４３０が直接アクセスし得ないローカルメモリリソースを含み得る。制御レジスタ４３１に関連して上述したように、ＣＰＵ４３０自体はまた、１つ又は複数のレベルのキャッシュメモリなどのローカルメモリリソースを含み得る。

【００３１】

また、ＳｏＣ４００の様々な周辺機能が、ＣＰＵ４３０によって及び互いにアクセス可能になるようにバスＭＡＢ及びＭＤＢに結合され得る。図３のアーキテクチャにおいて、これらの周辺機器は、ＳｏＣ４００の様々なメモリリソース、アナログ－デジタル（ＡＤＣ）及びデジタル－アナログ（ＤＡＣ）コンバータなどの様々な信号処理機能、通信ポート、タイマー、シリアル及びその他のインターフェース機能への、及びそれらからの、ダ

イレクトメモリアクセス（ＤＭＡ）アクセスを提供するためのＤＭＡエンジン４３３を含む。これらの様々な周辺機能は、バスＭＡＢ及びＭＤＢを介するアクセスしやすさによって示唆されるように、ＳｏＣ４００のアドレス空間内にあり得る。或いは、それらの又はその他の機能の１つ又は複数が、ＣＰＵ４３０により直接的に又は他の機能性回路要素を介してアクセスされ得る。また、セキュリティ特徴が、例えば、１つ又は複数のセキュアなメモリリソースにストアされたセキュリティパラメータと組み合わせたセキュアな状態機械４４８によってＳｏＣ４００内で実現され得、そのため、セキュアモードがイネーブルにされない限りセキュアな領域であると特定されるメモリ領域に対するデータの読出し又は書込みを禁止するなどの特徴が実行される。また、ＳｏＣ４００は、クロックシステム、並びに、デバッグ及びエミュレーションのためのエミュレーションシステム４２０及びＪＴＡＧインターフェース４２１など、他の機能を含む。

【００３２】

ＳｏＣ４００は、図３に示すものに付加的な又はそれらに代わる機能を含み得、または、示されたものと異なるアーキテクチャに従って配される機能を有し得る。

【００３３】

図４は、図３のＳｏＣ４００のアーキテクチャに組み込まれるなど、一実施形態に従ったＦＲＡＭサブシステムのアーキテクチャを示す。このアーキテクチャは、特に、ＦＲＡＭ４１０にストアされるファームウェアの更新の例に対して、ＦＲＡＭ４１０の内容の更新に関わる機能を含む。このアーキテクチャにおけるＦＲＡＭ４１０は、ＦＲＡＭコントローラ４１１からメモリアドレスを受け取るように、及び、ＦＲＡＭコントローラ４１１に及びＦＲＡＭコントローラ４１１からデータ及び制御信号を通信するように結合される。ＦＲＡＭコントローラ４１１は、ＣＰＵ４３０からメインアドレスバスＭＡＢを介してアドレスを受け取るように、及び、メインデータバスＭＤＢを介してＣＰＵ４３０とデータを通信するように結合される。また、ＣＰＵ４３０は、ＦＲＡＭコントローラ４１１内の制御レジスタに対応するメモリアドレスに制御情報を書き込むことなどによって、制御情報をバスＭＡＢ、ＭＤＢを介してＦＲＡＭコントローラ４１１に通信し得る。これ以降でさらに説明するように、ＦＲＡＭコントローラ４１１は、また、図４に示すように、キャッシュ４１１ｃの形態の内部メモリを含み得る。このキャッシュ４１１ｃは、通常動作の間のＦＲＡＭ４１０及びＳｏＣ４００におけるより高位のキャッシュ（例えば、ＦＲＡＭコントローラ４１１によってＦＲＡＭ４１０から既にリトリーブされたファームウェア命令のための命令キャッシュとして）の更新において用いられ得る。

【００３４】

この実施形態によれば、ＦＲＡＭコントローラ４１１からＦＲＡＭ４１０に通信される制御信号は、ＦＲＡＭ４１０の特定の動作モードを示す１つ又は複数の制御信号を含む。ＦＲＡＭ４１０は、感知アンプ、アドレスデコーダ、及びその他の従来の周辺回路要素（この例ではＦＲＡＭコントローラ４１１内に含まれない範囲で）とともに、図２ｂに関して前述したものなど、従来のように行及び列に配される強誘電メモリセルのアレイを含む。ただし、この実施形態では、ＦＲＡＭ４１０は、そのメモリセルが２トランジスタ２コンデンサ（２Ｔ２Ｃ）強誘電セルとして又は１トランジスタ１コンデンサ（１Ｔ１Ｃ）強誘電セルとして動作し得るように構築される。一般的な意味において、これ以降により詳細に説明されるように、ＦＲＡＭ４１０は、このセルアーキテクチャによって提供されるデータ保持及び優れた読出しマージンが得られるように、ＳｏＣ４００の通常動作モードにおいて２Ｔ２Ｃ強誘電メモリとして動作し得、このセルアーキテクチャによって提供される倍の容量が一時的に享受されるように、更新モードにおいて１Ｔ１Ｃメモリとして動作し得る。

【００３５】

本明細書において上述したように、従来のＦＲＡＭアレイ及び周辺回路要素は、２Ｔ２Ｃ又は１Ｔ１Ｃモードで選択的に動作し得る。図５は、この実施形態に関連して有用な構成を有する、上記で組み込まれた米国特許番号第５，７５１，６２８号の手法に従う例を図示する。２つの動作モード間で選択する能力は様々な方式で実装され得る。この例にお

いて、図５は、２Ｔ２Ｃ　ＦＲＡＭセル$2_{j,k}$のｍ行及びｎ列のアレイにおける列ｋの一部を図示する。ここで、ｊは、所与のセル$2_{j,k}$が存在するｍ個の２Ｔ２Ｃ行の１つを示す。アレイ全体には、同様に配されるＦＲＡＭセルの他の列も含まれる。各２Ｔ２Ｃセル$2_{j,k}$は第１及び第２のハーフセルを有し、第１及び第２のハーフセルは各々、従来のようにプレートラインＰＬとパストランジスタとの間に結合される強誘電コンデンサを含むように示されている。この例におけるこれら２つのハーフセルを、それぞれ、左及び右のハーフセル$2_{j,k}$［Ｌ］及び$2_{j,k}$［Ｒ］と称する。（２Ｔ２Ｃの意味における）相補的なビットラインＢＬＴ$_k$、ＢＬＣ$_k$が、列ｋにおける左右のセル２のパストランジスタに及び列ｋに対する感知アンプ４６$_k$に結合される。感知アンプ４６$_k$は、列ｋからの読出し動作においてビットラインＢＬＴ$_k$、ＢＬＣ$_k$における電圧の比較に応答してデータ状態信号（図示せず）を転送する従来の差動感知アンプである。ＦＲＡＭ４１０のセル２へのデータの書込みは、特定の動作モード（２Ｔ２Ｃ又は１Ｔ１Ｃ）に従って従来の方式で実施される。

【００３６】

この構造において、左ハーフセル$2_{j,k}$［Ｌ］及び右ハーフセル$2_{j,k}$［Ｒ］のパストランジスタは、それらのゲート電極で別々のワードラインを受ける。例えば、左ハーフセル$2_{0,k}$［Ｌ］は行デコーダ４０からワードラインＷＬ$_0$を受け、右ハーフセル$2_{0,k}$［Ｒ］はワードラインＷＬ$_0$を受ける。同様に、左ハーフセル$2_{j,k}$［Ｌ］は偶数番号のワードラインＷＬ$_2$、ＷＬ$_4$、．．．、ＷＬ$_{2m-4}$、ＷＬ$_{2m-2}$を受け、右ハーフセル$2_{j,k}$［Ｒ］は行デコーダ４０から奇数番号のワードラインＷＬ$_3$、ＷＬ$_5$、．．．、ＷＬ$_{2m-3}$、ＷＬ$_{2m-1}$を受ける。ＦＲＡＭコントローラ４１１は、或る行アドレスを行デコーダ４０に提供する。この行アドレスは、ｍ行の２Ｔ２Ｃセルの１つを選択し、選択された２Ｔ２Ｃ行の左ハーフセルと右ハーフセルとの間で選択し得る付加的な最下位ビットを有する。また、ＦＲＡＭコントローラ４１１は、ＦＲＡＭ４１０が１Ｔ１Ｃ又は２Ｔ２Ｃモードのいずれで動作するかを示す制御信号１Ｔ１Ｃ／$\overline{2T2C}$をこの例では行デコーダ４０に提供する。図４のＦＲＡＭサブシステムの構成は、どのＦＲＡＭコントローラ４１１が制御信号１Ｔ１Ｃ／$\overline{2T2C}$の適切な論理状態を所望の動作モードに対してＦＲＡＭ４１０に発行するかに応答して、適切な値をＦＲＡＭコントローラ４１１の制御レジスタにストアするＣＰＵ４３０によって設定される。２Ｔ２Ｃモードでの動作を示す制御信号１Ｔ１Ｃ／$\overline{2T2C}$に応答して、ワードライン信号の生成において行アドレスの最下位ビットが無視され、アクセスサイクルにおいて両方のワードライン（例えば、第１の行Ｊ＝０に対するワードラインＷＬ$_0$及びＷＬ$_1$）に通電されるように、ＬＳＢマスク４１が行デコーダ４０において設定される。逆に、１Ｔ１Ｃモードでは、ＬＳＢマスク４１はイネーブルされず、行アドレスの最下位ビットが信号ワードラインの選択に含まれる。ＦＲＡＭ４１０の所望の構成及び動作モードは、このように又は他の従来の手法に従って、容易に選択可能である。

【００３７】

また、この例示実装形態に従ったＦＲＡＭ４１０は、１Ｔ１Ｃモードで用いるための基準電圧生成器４４を含む。基準電圧生成器４４は、ＦＲＡＭ４１０の予期「０」ビットライン電圧と予期「１」ビットライン電圧との間のレベルの安定出力電圧を生成する従来の基準電圧回路とし得る。或いは、上記で組み込まれた特許第５，７５１，６２８号において説明されるように、基準電圧生成器４４は、所望の基準レベルのビットライン電圧を生成するようにサイズ設定又は分極される１対の強誘電コンデンサとして構築され得る。パストランジスタ42_0、42_1は、行デコーダ４０から、それぞれ、ダミーワードライン

ＤＷＬ０、ＤＷＬ１によって各々オンにされると、基準電圧生成器４４を、それぞれ、ビットラインＢＬＴ$_{k}$、ＢＬＣ$_{k}$に結合する。この例では、行デコーダ４０は、右ハーフセル２$_{j,k}$［Ｒ］を選択する行アドレスのＬＳＢ（すなわち、ＬＳＢ＝１）に応答して、基準電圧生成器４４をビットラインＢＬＴ$_{k}$に接続するためダミーワードラインＤＷＬ０を通電させ、左ハーフセル２$_{j,k}$［Ｌ］を選択する行アドレスのＬＳＢ（すなわち、ＬＳＢ＝０）に応答して、基準電圧生成器４４をビットラインＢＬＣ$_{k}$に接続するためダミーワードラインＤＷＬ１を通電させる。このようにして、感知アンプ４６$_{k}$は、１Ｔ１Ｃモードにおいて ＦＲＡＭ４１０を用いて列ｋにおける選択されるハーフセルのシングルエンド感知を実施する。

【００３８】

図６及び図７ａ～図７ｆを参照し、一実施形態に従った、ＳｏＣ４００などのＳｏＣデバイスにおけるＦＲＡＭサブシステムの動作を説明する。特に、このＦＲＡＭサブシステムの動作のこの例を、ＦＲＡＭ４１０にストアされるＳｏＣ４００のためのファームウェアの更新の文脈で説明する。これは、この実施形態がこのような応用例で用いられる場合に特に有益だからである。また、この同じプロセス及び動作は、システムファームウェア以外のＦＲＡＭメモリの内容を更新する際に有用である。図４のアーキテクチャにおいて、この更新プロセスは、主にＦＲＡＭコントローラ４１１によって、ＣＰＵ４３０の初期化及び指示において、例えば、更新の通信に対応する割込みによって呼び出される割込みハンドラルーチンなどにおいて、実行され制御される。更新に関わる特定のタスクやプロセスを司る特定の論理回路は、デバイスの特定のアーキテクチャ及びデバイスのＦＲＡＭリソースに応じて、この実装形態とは異なり得る。この実施形態は、このような応用例及び代替アーキテクチャに容易に適合され得る。

【００３９】

ファームウェア更新の文脈において、ＳｏＣファームウェアのオリジナルの又はその他の前のバージョンが、ＦＲＡＭ４１０に初期的にストアされ、そのオリジナルファームウェア又はより以前の更新の元でアプリケーションソフトウェアがＳｏＣ４００によって実行される又はその他の方式で実施される通常システム動作に対して用いられる。通常、ＳｏＣ４００のこの通常動作は、ＦＲＡＭ４１０を用いてその２Ｔ２Ｃモードにおいて、それに従ったＦＲＡＭコントローラ４１１の適切な制御レジスタの内容を設定したＣＰＵ４３０に応答して適切なレベルの制御信号１Ｔ１Ｃ／$\overline{2T2C}$を発行するＦＲＡＭコントローラ４１１によって実施される。上述したように、ＦＲＡＭ４１０のその２Ｔ２Ｃモードでの動作は、最適な読出しマージン及び確実なデータ保持性能での長期ストレージに適している。

【００４０】

図７ａは、オリジナルファームウェア内容を含むＦＲＡＭ４１０の一部の内容の例を、ＦＲＡＭ４１０の通常動作の間であり、ファームウェア更新を受ける前の状態で図示する。この例では、ＦＲＡＭ４１０内の２Ｔ２Ｃセルの８つの行が、オリジナルファームウェアコードをストアしているように示されている。図５に関して上述したように構築されるＦＲＡＭ４１０の２Ｔ２Ｃモードにおいて、これら８つの行は２Ｔ２Ｃ行アドレス０００ｘ～１１１ｘに対応する。ここで、「ｘ」は、左ハーフセルと右ハーフセルとの間で選択する最下位ビットが無視される（すなわち、行デコーダ４０のＬＳＢマスク４１によって「マスク」される）ことを示す。上述したような２Ｔ２Ｃ　ＦＲＡＭセルの差動動作のため、各右ハーフセル２$_{j,k}$［Ｒ］の分極状態は、対応する左ハーフセル２$_{j,k}$［Ｌ］の状態の論理相補である。したがって、オリジナルファームウェアコードは、一方のコピーが左ハーフセルにストアされ、他方のコピーが右ハーフセルに相補データとしてストアされるように、ＦＲＡＭ４１０において２つのコピーとしてストアされ得る。

【００４１】

従来、ＳｏＣ４００は、ＦＲＡＭ４１０にストアされたファームウェアに対する更新を

含む更新されたソフトウェアを、非同期で、又は、ユーザによる或いはホストネットワークノードからのファームウェア更新の初期化（「フラッシュ」）の際に、受け取り得る。本実施形態において、ＳｏＣ４更新されたファームウェアの指示を００が受けると、ファームウェア更新割込みが呼び出され、本実施形態に従って図６の割込みハンドラルーチンが実行される。

【００４２】

本実施形態によれば、ファームウェア更新割込みハンドラはプロセス５６で開始する。プロセス５６において、ＦＲＡＭコントローラ４１１がＦＲＡＭ４１０を更新モードにする。これらの実施形態において、プロセス５６において入る更新モードにより、ＦＲＡＭ４１０が、セル２を１Ｔ１Ｃ　ＦＲＡＭセルとみなして動作させ、行デコーダ４０、感知アンプ４６、及びＦＲＡＭ４１０の他の周辺回路要素を、１Ｔ１Ｃ　ＦＲＡＭに適切なように動作させる。例えば、図５のアーキテクチャにおいて、行デコーダ４０のＬＳＢマスク４１がイナクティブにされて、行アドレスの最下位ビットの値に応答して各サイクルにおいてダミーワードラインＷＬ０、ＤＷＬ１の一方がアクティブにされる。図７ｂを参照すると、図７ａに示すようなＦＲＡＭ４１０の２Ｔ２Ｃ行はここでは、ハーフ行の対、又は、最下位行アドレスビットの状態に基づいて選択可能であり、互いに相補的なデータをストアする１Ｔ１Ｃ行、とみなされる。例えば、１Ｔ１Ｃ行アドレス００００が、第１の２Ｔ２Ｃ行ｊ＝０００ｘの左ハーフセル$2_{0,k}$［Ｌ］に対応し、１Ｔ１Ｃ行アドレス０００１が、第１の２Ｔ２Ｃ行ｊ＝０００ｘの右ハーフセル$2_{0,k}$［Ｒ］に対応する。１Ｔ１Ｃ行０００１にストアされたデータは、１Ｔ１Ｃ行００００にストアされたデータの論理相補である。１Ｔ１Ｃ行を交互にすることによるこの相補データは、図７ｂに示すようにＦＲＡＭ４１０を通して続く。本質的に、ＦＲＡＭ４１０のメモリ容量は、２Ｔ２Ｃモードと比較するとこの１Ｔ１Ｃモードにおいて倍であるが、このプロセスのこの時点において、同じデータの２つのコピーをストアしている。

【００４３】

任意選択で、プロセス５６においてＦＲＡＭ４１０を１Ｔ１Ｃモードにする前に、ＦＲＡＭ４１０にストアされたオリジナルデータは、読み出すこと、次いでアレイ内の各セルに同じデータ再書き込みすることによって「リフレッシュ」され得る。後続の動作が１Ｔ１Ｃモードでのシングルエンド感知のこれらのストアされた内容を読み出すことを考慮すると、ＦＲＡＭ４１０の内容のこのリフレッシュは、ストアされたデータのビット毎に全分極状態を再確立するために有用であり得る。所望とされる場合、このリフレッシュは、ストアされたデータに対する分極状態を大きくするため、何らかのＦＲＡＭテスト動作やモードで用いられるなどの、高められた電力供給電圧で成され得る。

【００４４】

プロセス５８において、ＳｏＣ４００のための更新されたファームウェアに対応する新たなデータが、受け取られ、ＦＲＡＭ４１０内の各ＦＲＡＭセル２の一方の側のハーフセルに書き込まれる。この例では、これらの更新されたデータは、ＦＲＡＭ４１０の右ハーフセルに、図７ｃに示すように、最下位行アドレスビットにおいて「１」を有する１Ｔ１Ｃ行に（すなわち、行アドレス$a_3a_2a_1$１で）ストアされる。１Ｔ１Ｃモードに切り換えることによってＦＲＡＭ４１０の容量が効果的に倍になることにより、本質的に、ファームウェア更新及び他の新たなデータを受け取るフルサイズバッファが、ＳｏＣ４００においてそのバッファのための付加的なメモリセルを必要とすることなく、提供される。更新されたファームウェアは、必ずしも、交互の１Ｔ１Ｃ行によって提供される利用可能なバッファを満たす必要はない。

【００４５】

プロセス５８における更新されたデータの交互の１Ｔ１Ｃ行への書込みは様々な方式で成され得る。この例では、更新されたデータは各列ｋの相補ビットラインBLC_kに関連する右ハーフセルに書き込まれるので、これらの更新されたデータは、実際の更新されたデータの論理相補として書き込まれ得る。或いは、これらのデータは、真のデータ状態として（すなわち、受け取られたように）右ハーフセルに書き込まれ得る。更新されたデー

タは、代わりに、プロセス５８において左ハーフセルに書き込まれてもよく、より以前のバージョンが右ハーフセルに保持される。いずれの場合も、後続のプロセスにおいて、これらのデータの真の状態又は相補状態が把握され得る。また、プロセス５８の実際の書込みサイクルは、２Ｔ２Ｃセルに比して、１Ｔ１Ｃ　ＦＲＡＭセルによって本質的に提供される低減された読出しマージンに照らして、ストアされたデータに対する分極状態を大きくするため、何らかのＦＲＡＭテスト動作やモードで用いられる値など、高められた電力供給電圧で成され得る。

【００４６】

プロセス５８における更新されたデータ（例えばファームウェア）の交互の１Ｔ１Ｃ行への書込みに続き、これらの更新されたデータは、更新されたデータが正確に受け取られストアされることを保証するため、プロセス６０においてＣＰＵ４３０によって適切な方式で検証される。この実施形態によれば、検証プロセス６０は、ＣＰＵ４３０よって実施されるか、又はストアされた更新されたデータに対して何らかのタイプの数値データ検証ルーチンを実行する、ＳｏＣ４００における別の論理回路によって実施され得る。プロセス６０において、様々な従来の数値データ検証技術（巡回冗長検査（ＣＲＣ）、ハッシュ、暗号ハッシュ、及びチェックサムの評価など）が有用である。この検証は通常、データがプロセス５８でストアされた交互の行（図７ｃの行アドレス$a_3a_2a_1$１）からの更新されたデータのＦＲＡＭコントローラ４１１によるリトリーブに関与し、所望に応じて、ＣＰＵ４３０又はＳｏＣ４００におけるその他の演算ロジックによる適切な検証計算の実行に関与する。

【００４７】

判定６１において、プロセス６０の検証が成功したか否かが判定される。成功判定は、ＦＲＡＭ４１０の交互の行に書き込まれた更新されたデータに誤りがなく（又は、少なくとも従来の誤り補正を用いて補正され得）、真であり正確であるとして信頼され得ることを示す。この場合（判定６１で「Ｙｅｓ」）、これらの更新されたデータは、プロセス６２において、ＦＲＡＭ４１０の対になった交互の行にコピーされ、これらの場所のオリジナルデータに上書きされる。ＦＲＡＭ４１０は、このプロセス６２に対し依然として１Ｔ１Ｃ更新モードである。図７ｄに示すように、プロセス６２の上書きは、所与の２Ｔ２Ｃ行（例えば、行アドレス０００１）の右ハーフセルにストアされたデータをリトリーブし、それらの同じデータが同じ２Ｔ２Ｃ行の左ハーフセルに（例えば、行アドレス００００に）書き込まれる。プロセス６２のこの上書きは、更新されたファームウェア又は他のデータを含む、ＦＲＡＭ４１０の他の行すべてについて実施される。この例では、各行アドレス$a_3a_2a_1$１における内容は、対になった行アドレス$a_3a_2a_1$０におけるセルにコピーされる。好ましくは、プロセス６２の上書きは、更新されたデータの論理相補を対応する交互の１Ｔ１Ｃ行に書き込み、そのため、行$a_3a_2a_1$０にストアされたデータが、その対照行$a_3a_2a_1$１にストアされたデータの論理相補となるようにする。図５のアーキテクチャでは、相補的なストアされたデータの極性が、左ハーフセルが「真」のビットラインBLT_kに関連付けられ、右ハーフセルが「相補」ビットラインBLC_kに関連付けられるという慣行と調和していると好都合となり得る。また、プロセス６２の実際の書込みサイクルは、２Ｔ２Ｃセルに比して１Ｔ１Ｃ　ＦＲＡＭセルによって本質的に提供される低減された読出しマージンを考慮して、ストアされたデータに対する分極状態を大きくするため、何らかのＦＲＡＭテスト動作やモードで用いられる値など、高められた電力供給電圧で実施され得る。

【００４８】

プロセス６２における交互の１Ｔ１Ｃ行（例えば、アドレス$a_3a_2a_1$１）から対になった交互の行アドレス（$a_3a_2a_1$０）への更新されたデータのコピーは、ＳｏＣ４００におけるハードウェア機能によって成され得る。例えば、図４のアーキテクチャを参照すると、この上書きを行なうためのハードウェア手法の一つは、ＣＰＵ４３０に関与することなく、ＦＲＡＭ４１０を読み出すため、及び相補データをＦＲＡＭ４１０に再書き込みするために、ＦＲＡＭコントローラ４１１を用いることである。この手法では、プロ

セス６２においてＦＲＡＭ４１０からリトリーブされた内容を一時的にストアするためにキャッシュ４１１ｃが用いられ得、そのため、ＦＲＡＭ４１０からのＦＲＡＭ４１０へのより大きなデータブロックの読出し及び書込みが可能になる。別のハードウェアベースの手法が、ＣＰＵ４３０に関与することなく、ＦＲＡＭ４１０の交互の１Ｔ１Ｃ行（例えば、アドレス$a_3a_2a_1$1）から内容をリトリーブするため、及びこれらの内容を対になった交互の行アドレス（$a_3a_2a_1$0）に再書き込みするために、ＤＭＡエンジン４３３を用い得る。或いは、プロセス６２は、ＢＳＬ　ＲＯＭ４３２から又はＦＲＡＭ４１２自体からフェッチされるものなどのソフトウェア命令を実行するＣＰＵ４３０によって成され得、そのため、交互の行からの内容の、対応する対になった行へのコピーに関与する読出し及び書込みが実施されるようにする。これら及びその他の手法のうちの適切な手法が、特定の応用例及びアーキテクチャに適切なように、これら及びその他のハードウェアとソフトウェアベース技術のハイブリッドを含めて、容易に実装され得る。

【００４９】

プロセス６２において成された更新されたデータのコピーに続き、プロセス７０において、ＦＲＡＭコントローラ４１１が、ＦＲＡＭ４１０を２Ｔ２Ｃモードにするために適切なレベルの制御信号１Ｔ１Ｃ／$\overline{2T2C}$を発行することによってこの実施形態に従った更新プロセスが終了し、これに続いて、割込みから戻り、更新されたファームウェアの下で通常動作モードでの動作が開始する。再び、２Ｔ２ＣモードでのＦＲＡＭ４１０を用いて、セル２が、行デコーダ４０のＬＳＢマスク４１によって最下位ビットがマスクされる行アドレス$a_3a_2a_1$ｘによって行毎にアクセスされ、そのためこの２Ｔ２Ｃモードでの行アドレスのデコードにおいて最下位ビットが無視される。次いで、ＳｏＣ４００の適切なアプリケーションが実行が再び成される。

【００５０】

比較として、プロセス６０において成された更新されたデータ（例えばファームウェア）の検証が不成功である場合、判定６１は「Ｎｏ」の結果を戻し、更新されたファームウェアに１つ又は複数の補正不可能な誤りが検出されたことを示す。このような誤りは、ネットワークリンクを介する更新の通信において、或いはＦＲＡＭ４１０による更新されたデータのストレージ又は保持において生じ得る。この事象において、この失敗が更新のソースに通知するためプロセス６６が実行され、所望の場合はこの更新が再送信される。ＦＲＡＭ４１０の交互の行にストアされた更新されたデータは、無効とみなされ、ＦＲＡＭ４１０の交互の１Ｔ１Ｃ行（例えば、アドレス$a_3a_2a_1$1）から対になった交互の行アドレス（$a_3a_2a_1$0）に上書きコピーされない。そうではなく、プロセス６８において、より以前のバージョンをストアするＦＲＡＭ４１０の１Ｔ１Ｃ行から（例えば、行アドレス$a_3a_2a_1$0から）失敗した更新を受け取った交互の行アドレス（$a_3a_2a_1$1）のセルに古いデータが上書きコピーされる。ＦＲＡＭ４１０はこのプロセス６８では１Ｔ１Ｃ更新モードのままである。プロセス６８において書き込まれる特定のデータ状態は、この場合も、上述の差動データのストア及び２Ｔ２Ｃ　ＦＲＡＭの感知と一貫して、古いデータがリトリーブされる対応するアドレスのデータ状態の相補である。プロセス６８のこの上書きは、上述のように、ストアされたデータの信頼性を最適化するため、高められた電圧で成され得、ＳｏＣ４００における特定のハードウェア又はＤＭＡロジックによって、或いは、ＣＰＵ４３０、又はこのプロセス６８を行なうためのソフトウェアルーチンを実行するその他の論理回路要素によって、成され得る。図７ｆは、プロセス６８における古いデータの上書きを図示する。このプロセス６８で成されるような、より以前のバージョンのストアされたデータの置換えに続いて、プロセス７０において、ＦＲＡＭコントローラ４１１は、ＦＲＡＭ４１０を２Ｔ２Ｃモードにするために適切なレベルの制御信号１Ｔ１Ｃ／

$\overline{2T2C}$

を発行し、ファームウェア更新割込みハンドラから戻る。次いで、ＳｏＣ４００の通常動作が継続され得、更新されたファームウェア又はその他のデータのソースエンドからの再送信を、もしそういったことが成される場合、待機する。

【００５１】

これらの実施形態は、埋込み不揮発性メモリを含む集積回路において、更新されたファームウェア及びその他のプログラムコード又はデータを効率的に受け取り検証する能力を提供する。この能力は、強誘電メモリを、その２Ｔ２Ｃ動作モードから、倍の容量であるが信頼性が低い１Ｔ１Ｃ動作モードに、受け取った更新されたデータを検証しコピーするために必要とされる時間にわたって、一時的に再構成することによって提供される。この手法は、差動データストア及び２Ｔ２Ｃ　ＦＲＡＭメモリの感知によって提供される、確実な読出しマージン性能及び優れたデータ保持を保つ。これは、システムファームウェア内に一般に含まれるシステムソフトウェアルーチンをストアするためによく適しており、１Ｔ１Ｃ　ＦＲＡＭメモリの倍ビット密度は、更新及び検証プロセスにおいて有利に用いられる。したがって、集積回路自体内の、又は、全システムにおける外部メモリデバイスとしての、検証を介するファームウェア更新を受けるための付加的なバッファが必要とされず、大規模集積回路及びそれが実装されるシステムのコスト及び電力消費が低減される。

【００５２】

本明細書から明らかなように、これらの実施形態は、強誘電メモリ技術を用いて構築されるように上記で説明されている。代替として、これらの実施形態は、類似の構造ではあるが、強誘電材料の分極以外の不揮発性ストレージ技術を用いるメモリにおいて実装され得る。例えば、これらの実施形態は、１つのモードにおいて差動感知のために別々の導体（例えばビットライン）に結合されるが、別の動作モードにおいてそれらのビットラインを介して別々に書き込み及び感知され得る、１対の磁歪ランダムアクセスメモリ（ＭＲＡＭ）ストレージ要素を含むメモリセルを用いて実現され得る。

【００５３】

特許請求の範囲内で、説明した実施形態の改変が可能であり、他の実施形態が可能である。

【図１】

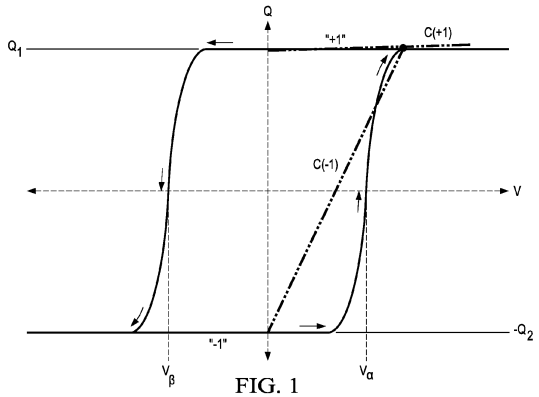

FIG. 1
（従来技術）

【図２ａ】

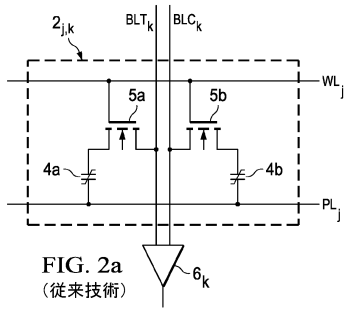

FIG. 2a
（従来技術）

【図２ｂ】

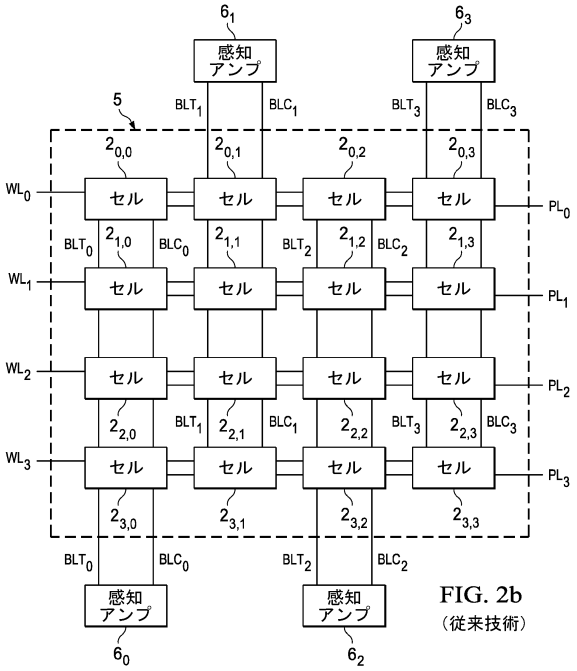

FIG. 2b
（従来技術）

【図２ｃ】

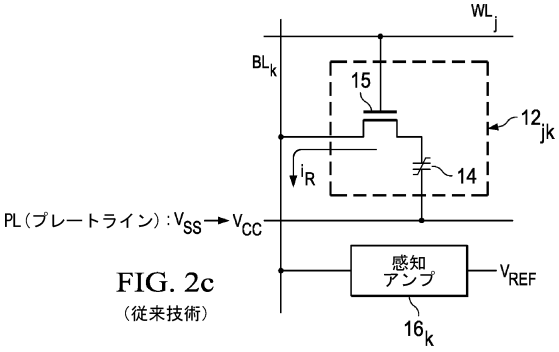

FIG. 2c
（従来技術）

【図３】

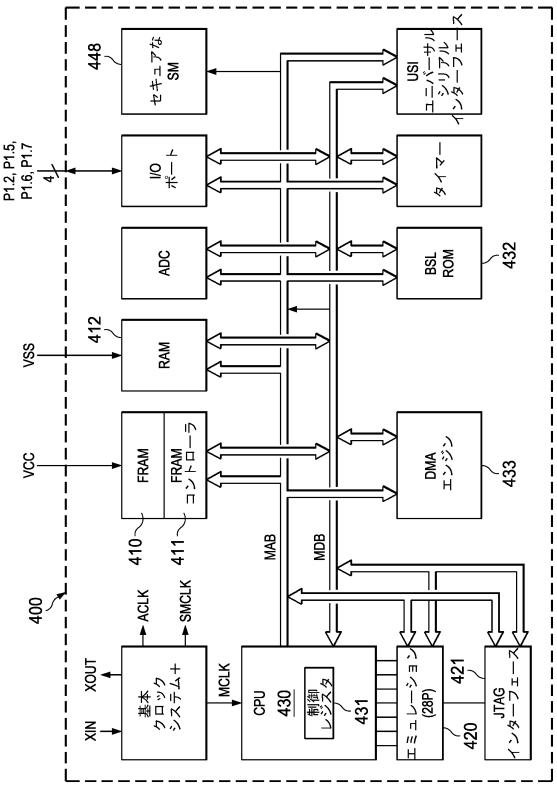

FIG. 3

【図４】

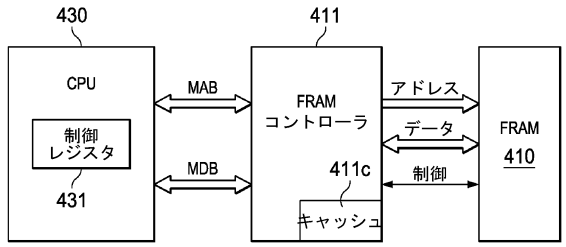

FIG. 4

【図５】

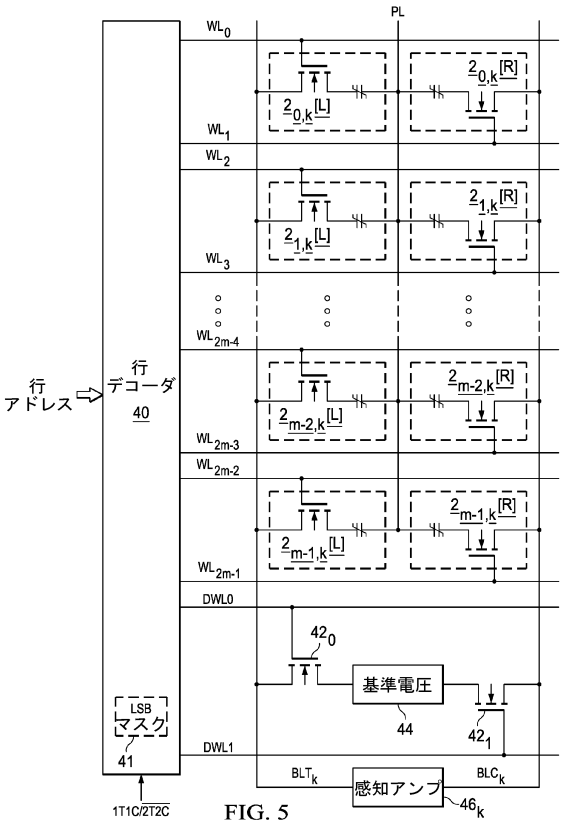

FIG. 5

【図６】

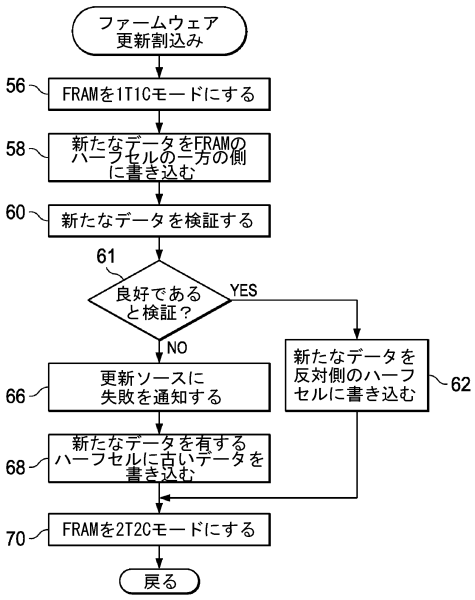

FIG. 6

【図７ａ】

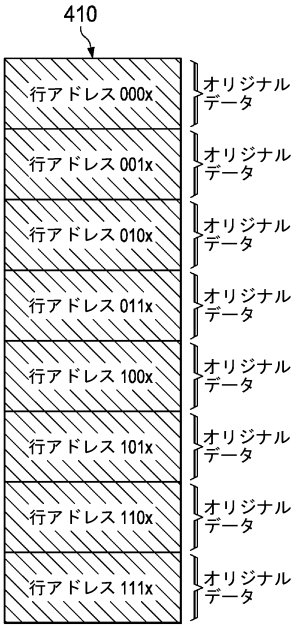

FIG. 7a

【図７ｂ】

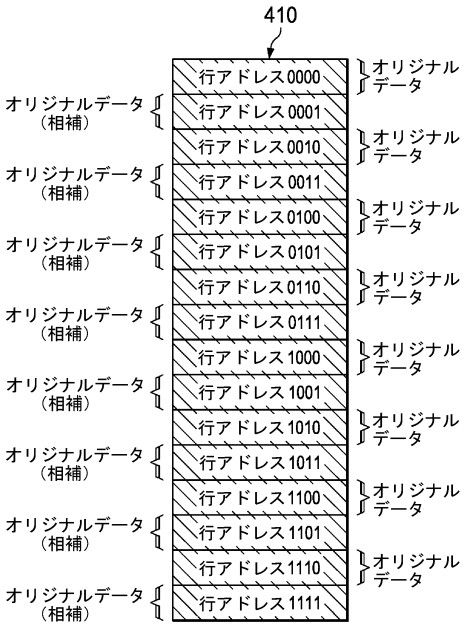

FIG. 7b

【図７ｃ】

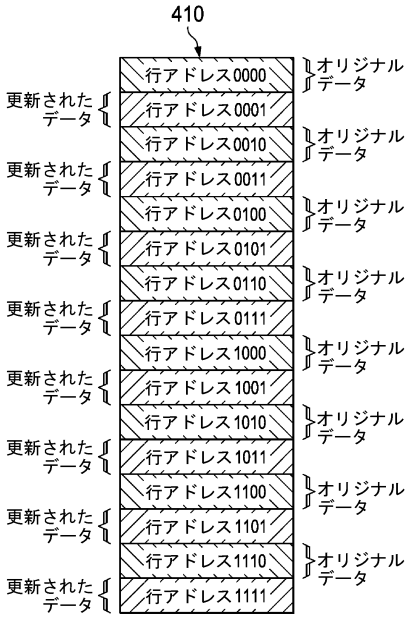

FIG. 7c

【図７ｄ】

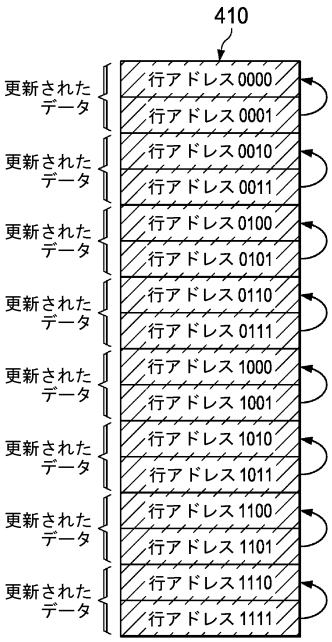

FIG. 7d

【図７ｅ】

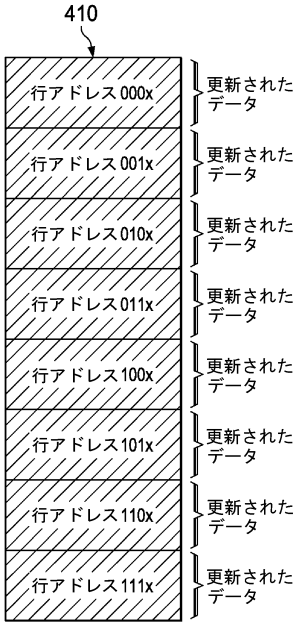

FIG. 7e

【図７ｆ】

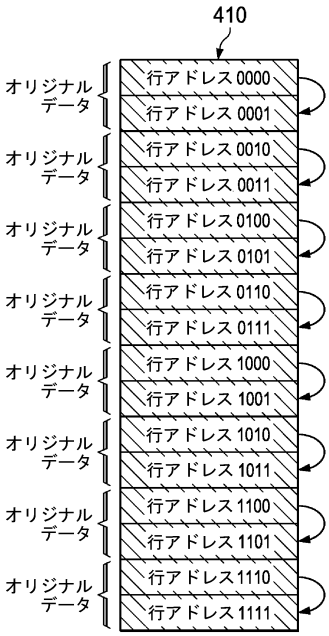
410
オリジナルデータ
行アドレス 0000
行アドレス 0001
オリジナルデータ
行アドレス 0010
行アドレス 0011
オリジナルデータ
行アドレス 0100
行アドレス 0101
オリジナルデータ
行アドレス 0110
行アドレス 0111
オリジナルデータ
行アドレス 1000
行アドレス 1001
オリジナルデータ
行アドレス 1010
行アドレス 1011
オリジナルデータ
行アドレス 1100
行アドレス 1101
オリジナルデータ
行アドレス 1110
行アドレス 1111

FIG. 7f

フロントページの続き

(74)上記2名の代理人 100098497
弁理士 片寄 恭三
(72)発明者 ラルフ ブレデロー
ドイツ連邦共和国 ポイング ８５５３６, ズデーテンシュトラーセ ５１
(72)発明者 オスカー ミゲル ギリェンエルナンデス
ドイツ連邦共和国 ミュンヘン ８０７９６, ヘルツォークシュトラーセ １０５
(72)発明者 ペーター ウォンゲウン チュン
アメリカ合衆国 ７５０３５ テキサス州 フリスコ, キャムデン レーン １５０８０

審査官 後藤 彰

(56)参考文献 特開２００５－９２９１５（ＪＰ, Ａ）
特開平１０－７９１９６（ＪＰ, Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ１１Ｃ １１／２２
Ｇ０６Ｆ ８／６５４