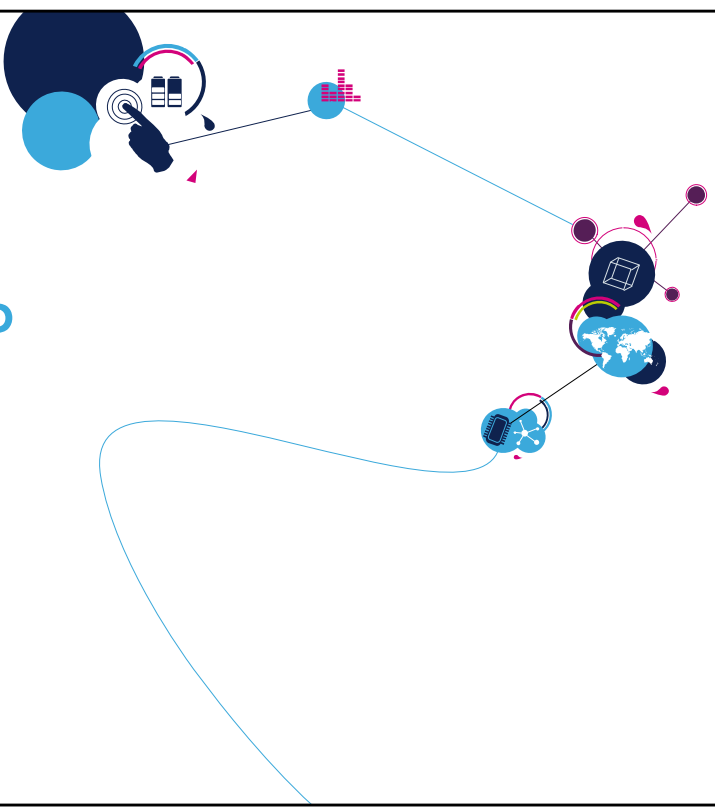




STM32G0 - TAMP

タンパおよびバックアップレジスタ

レビジョン 1.0



STM32 タンパおよびバックアップレジスタのプレゼンテーションへようこそ。ここでは、タンパイベントに対するセキュリティを確保するために使用されているこのペリフェラルの主な機能について説明します。

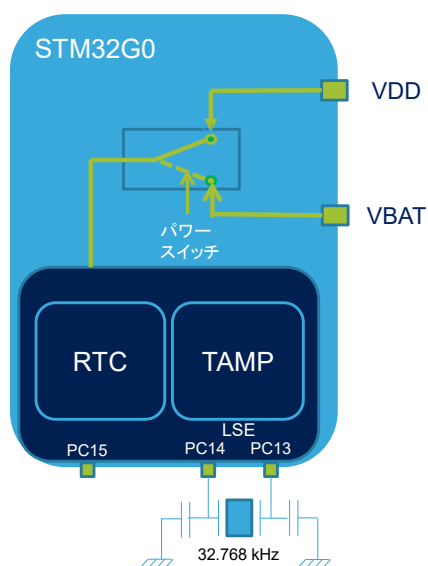
STM32F0との主な違い

2

- STM32F0マイクロコントローラとの主な違いは、内部タンパチャネルの導入である
- TAMPブロックとRTCブロックの分離、バックアップ・レジスタは引き続きTAMPブロックの一部である



STM32G0 には、タンパ検出ペリフェラル(TAMP)とリアルタイムクロック(RTC)という 2 つの別個のユニットが存在します。TAMP ブロックには、バックアップレジスタが含まれています。STM32F0 では、1 つのブロックだけでタンパと RTC の両方のユニットを処理します。



- TAMPは5つのバックアップ・レジスタを備えており、これらはタンパ検出時に消去される
- 2種類のタンパ入力: 外部 (2つGPIO) と内部 (4つのソース)
- バッテリ・バックアップ・ドメインに属しているため、メイン電源がオフのときにも機能する

アプリケーション側の利点

- タンパ保護されたバックアップ・レジスタ
- フィルタリングによる超低消費電力のタンパ検出



TAMP ペリフェラルは、メイン電源がオフのときにデータを保持するために使用される 5 つの 32 ビットバックアップレジスタを備えています。これらのバックアップレジスタは、タンパピンまたは一部の内部イベントでタンパイベントが検出されたときに消去されるため、セキュアなデータを格納するために使用できます。

VBAT ドメインがバックアップバッテリーによって供給される場合、タンパ検出は低消費電力モードで機能します。

耐タンパ回路には、超低消費電力デジタルフィルタリングが含まれており、誤ったタンパ検出を回避します。

- 5 個のバックアップ・レジスタ:
 - バックアップ・レジスタ(TAMP_BKP0-4R)は、VDD電源が遮断された場合に VBA によって電源が供給される、バッテリー・バックアップ・ドメインに搭載されている
- 2個の外部タンパ検出イベント
 - 外部のパッシブ・タンパは、フィルタおよび内部プルアップが設定可能
- 4個の内部タンパイベント
- タンパ検出によってRTCタイムスタンプ・イベントを生成可能。
- 内部タンパ検出によってバックアップ・レジスタを消去
 - 外部タンパに関しては、消去を無効にすることも可能



TAMP の主な機能は次の通りです。

20 バイトのバックアップレジスタは、5 つの 32 ビットバックアップレジスタに分けられます。これらのレジスタは、すべての低消費電力モードおよび VBAT モードで保持され、2 個のタンパピンのいずれかまたは 4 個の内部タンパイベントでタンパ検出イベントが発生すると消去されます。 外部タンパイベントに関しては、ソフトウェアで、タンパイベントが検出されたときにバックアップレジスタを消去するかどうかを選択できます。

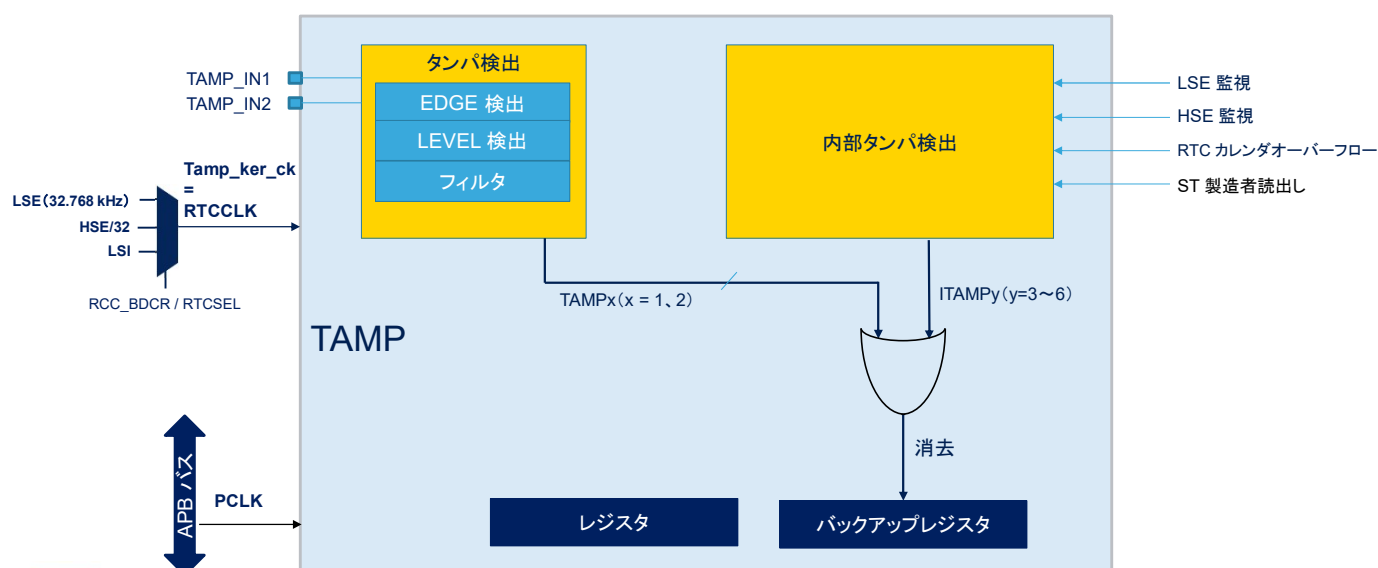
VBAT モードでは 2 本のタンパピンを使用できます。

外部タンパイベントは、プログラム可能なエッジ、またはレベルで検出することができます。レベルで検出する場合、超低消費電力モードで設定可能なフィルタと内部プルアップを使用します。

タイムスタンプ機能は、タンパイベントに応じて、タイムスタンプレジスタにカレンダーの内容を保存するために使用されます。

ブロック図

5

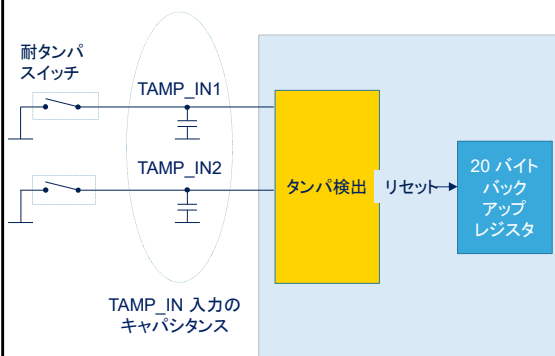


これは、TAMP のブロック図です。TAMP には 2 個のクロックソースがあります。TAMP クロック(RTCCLK)は、フィルタリングを使用したレベル検出モードでのタンパ検出にのみ使用され、APB クロックは TAMP およびバックアップレジスタの読出しおよび書込みアクセスに使用されます。タンパエッジ検出または内部タンパ検出には、クロックは必要ありません。TAMP クロックは、32 分周された高速外部オシレータ(HSE)、低速外部オシレータ(LSE)、または低速内部オシレータ(LSI)のいずれかを使用できます。STOP モードと STANDBY モードでは LSE または LSI のみが機能します。SHUTDOWN モードと VBAT モードでは LSE のみが機能します。

LSE 監視、HSE 監視、RTC カレンダオーバーフロー、ST 製造者読出しなど、いくつかの内部機能は、タンパイベントを生成できます。

デフォルトでは、すべてのタンパ検出イベントによってバックアップレジスタが消去されます。

超低消費電力耐タンパ回路



- 2個のタンパピンとイベントがVBATモードで使用可能
- イベントごとにアクティブなエッジまたはレベルを設定可能
- 外部タンパ・イベントが検出された場合にバックアップ・レジスタをリセット
 - 無効にできる
- タンパによってタイムスタンプ・イベントを生成可能



TAMP には、超低消費電力のタンパ検出回路が内蔵されています。その目的は、セキュアなアプリケーションで物理的なタンパを検出し、侵入が発生した場合に機密データを自動的に消去することです。2 個のタンパピンとイベントがサポートされており、すべての低消費電力モードおよび VBAT モードで機能します。

検出はエッジトリガまたはレベルトリガで、アクティブなエッジまたはレベルはイベントごとに設定可能です。

プリチャージ時間は、TAMP_INx 入力で大きなキャパシタンスをサポートするために、TAMPRECH ビットによって決定されます。

タンパイベントによってタイムスタンプイベントを生成でき、侵入の試みの日付を記録するために使用できます。

図に示すコンデンサによってフィルタリングが行われます。外部コンデンサがタンパ入力に明示的に接続されていない場合、トレース容量のモデルを提供します。

エッジ検出モードでは、外部プルアップが必要であることに注意してください。

レベル検出モードでは、次のスライドで説明されているように内部プルアップが使用されます。

フィルタリングによる安全で超低消費電力のタンパ検出

- 耐タンパスイッチの開状態を検出するようにI/Oプルアップ抵抗の使用を設定可能
- 異なるキャパシタンス値をサポートするようにプリチャージ・パルスを設定可能
 - 1、2、4、8サイクル
- フィルタを設定可能
 - サンプリングレート: 128、64、32、16、8、4、2、1Hz
 - マイクロコントローラをウェイクアップさせるための割込みを発行する前の、連続する同一イベントの数: 1、2、4、8



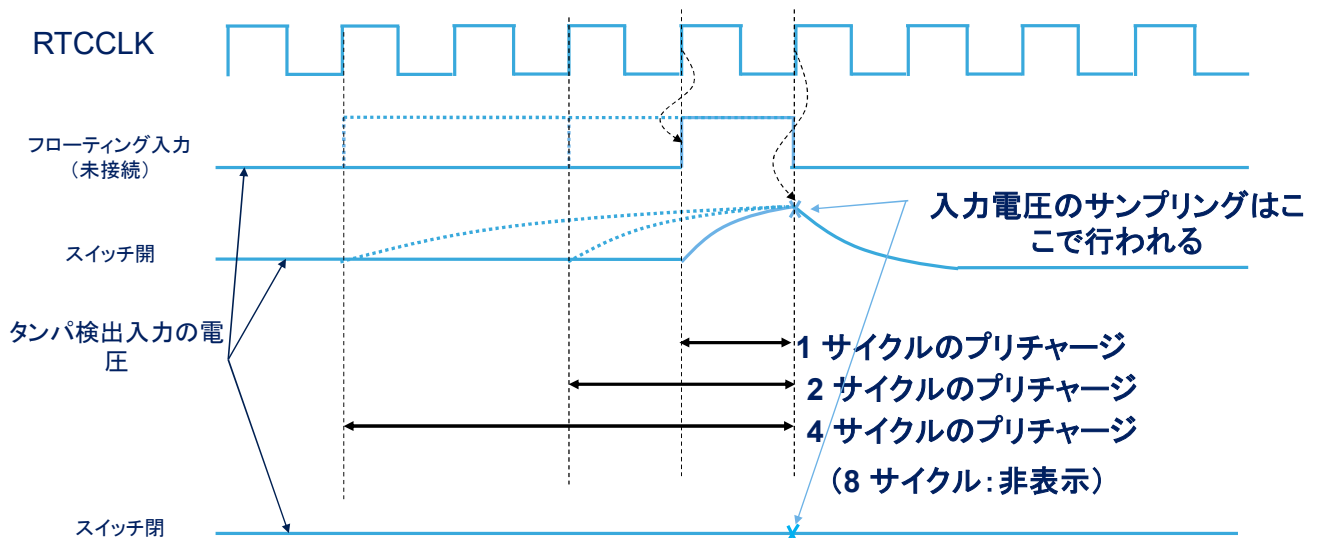
タンパ検出回路は、超低消費電力デジタルフィルタを備えています。内部 I/O プルアップを使用して、耐タンパスイッチの状態を検出できます。

I/O プルアップは、タンパピンがローレベルになった場合の電力消費を回避するためにプリチャージパルス中にのみ適用されます。プリチャージパルスの継続時間は、異なるキャパシタンス値をサポートするように設定可能で、1、2、4、8 TAMP クロックサイクルに設定できます。ピンレベルは、プリチャージパルスの最後にサンプリングされます。

タンパピンには、フィルタを適用できます。フィルタは、デバイスをウェイクアップさせるための割込みを発行する前に、特定の数の連続する同一イベントを検出することで構成されます。この数値は設定可能で、1～128 Hz のプログラム可能なサンプリングレートで 1、2、4、8 個のイベントを設定できます。

タンパ検出 - 信号

8



この図では、内部プルアップを使用したタンパ検出を示しています。内部プルアップは、1、2、4、または 8 サイクルに適用できます。スイッチを開いている場合、レベルは抵抗によってプルアップされます。スイッチを閉じている場合、レベルはローのままになります。

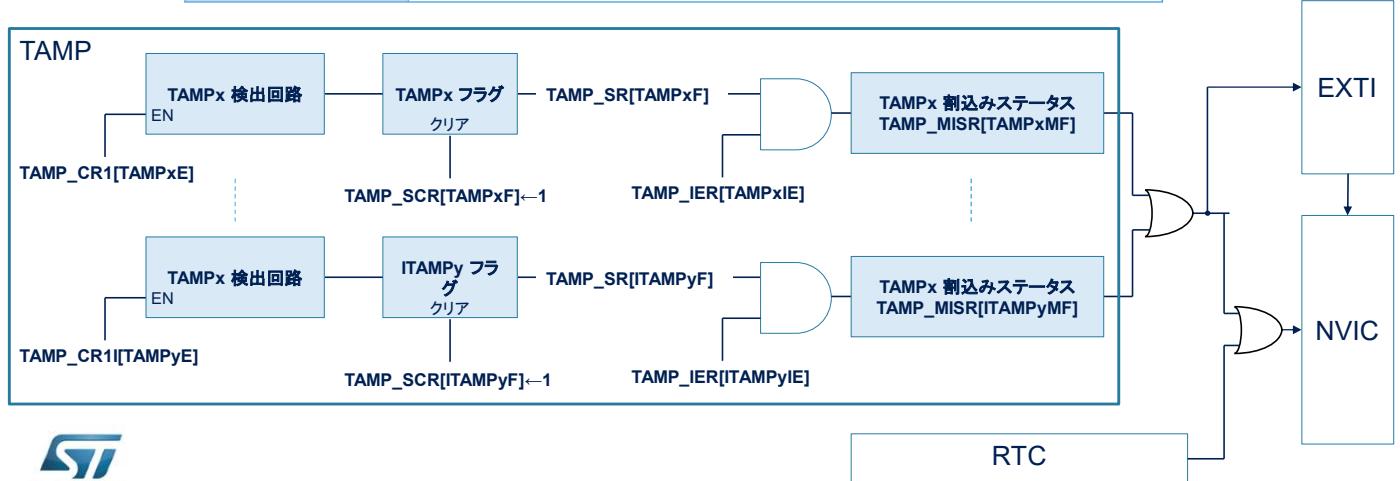
入力電圧は、プリチャージパルスの最後にサンプリングされます。

- タンパ検出は、割込みやトリガ・イベントを生成することができ、デジタル・フィルタリングの恩恵を受けることができる
 - 割込みは、イベントごとに有効／無効にできる
 - バックアップ・レジスタの消去は、外部イベントごとに設定可能
 - 低消費電力タイマへのハードウェア・トリガは、外部イベントごとに設定可能



タンパ検出回路は、割込みやトリガイベントの生成にも使用できます。各タンパ割込みは、個別に有効または無効にすることができます。外部タンパイベントごとに、バックアップレジスタを消去するかしないかを個別に設定できます。外部タンパイベントごとに、低消費電力タイマへのハードウェアトリガを生成するように個別に設定できます。これにより、割込みやトリガを生成する際に、これらの I/O に存在するデジタルフィルタリングを利用できます。

割込みイベント	説明
TAMPx	TAMP_INx ピンでタンパ・イベントが検出されたときにセット
ITAMPy	ITAMP_INy ピンで内部タンパ・イベントが検出されたときにセット



すべての割込みは、すべての低消費電力モードからプロセッサをウェイクアップできます。すべてのタンパピンと内部タンパソースの検出は、割込みを生成できます。

タンパ検出回路は、TAMP_CR1 レジスタをプログラミングすることによって有効または無効にできます。

このオプションが有効で、タンパイベントが検出された場合、TAMP_SR レジスタの対応するフラグがセットされます。

次に TAMP_IER レジスタは、タンパイベント割込みをマスクまたは有効にします。

割込みサービスルーチンは、タンパイベント割込みの原因を識別するフラグを含む TAMP_MISR レジスタを読み出すことによって、どのタンパイベントが発生したかを簡単に判断できます。

ネスト化されたベクタ割込みコントローラ(NVIC)には、RTC および TAMP モジュールに関連する固有の入力があります。

すべてのタンパ割込みリクエストを結合した OR ゲートの出力は、ダイレクトラインタイプとして拡張割込みコントローラ(EXTI)にも接続されます。これは CPU イベントウェイクアップ信号を生成したり、システムとコアのウェイクアップをリクエストしたりするために必要です。

低消費電力モード

11

モード	説明
RUN	アクティブ。
SLEEP	アクティブ。TAMP割込みによって、デバイスはSLEEPモードを終了する。
低消費電力 RUN	アクティブ。
低消費電力 SLEEP	アクティブ。TAMP割込みによって、デバイスは低消費電力SLEEPモードを終了する。
STOP 0/STOP 1	フィルタリングによるレベル検出は、LSEまたはLSIからクロックを供給された場合にのみアクティブになる。TAMP割込みによって、デバイスはSTOP 0/STOP 1モードを終了する。
STANDBY	フィルタリングによるレベル検出は、LSEまたはLSIからクロックを供給された場合にのみアクティブになる。TAMP割込みによって、デバイスはSTANDBYモードを終了する。
SHUTDOWN	フィルタリングによるレベル検出は、LSEからクロックを供給された場合にのみアクティブになる。TAMP割込みによって、デバイスはSHUTDOWNモードを終了する。



TAMP ペリフェラルはすべての低消費電力モードでアクティブであり、TAMP 割込みによってデバイスは低消費電力モードを終了します。STOP 0、STOP 1、および STANDBY モードでは、LSE または LSI クロックのみを使用して TAMP にクロックを供給できます。SHUTDOWN モードでは LSE のみが機能します。

- 次のTAMPにリンクされているペリフェラル・トレーニングを参照
 - リアルタイム・クロック(RTC)
 - リセットおよびクロック制御(RCC)
 - 電源制御(PWR)
 - 拡張割込みコントローラ(EXTI)
 - ネスト化されたベクタ割込みコントローラ(NVIC)



これは、リアルタイムクロックに関連するペリフェラルのリストです。詳細については、必要に応じてこれらのペリフェラルトレーニングを参照してください。

- リアルタイムクロック
- リセットおよびクロック制御
- 電源制御
- 拡張割込みコントローラ
- ネスト化されたベクタ割込みコントローラ