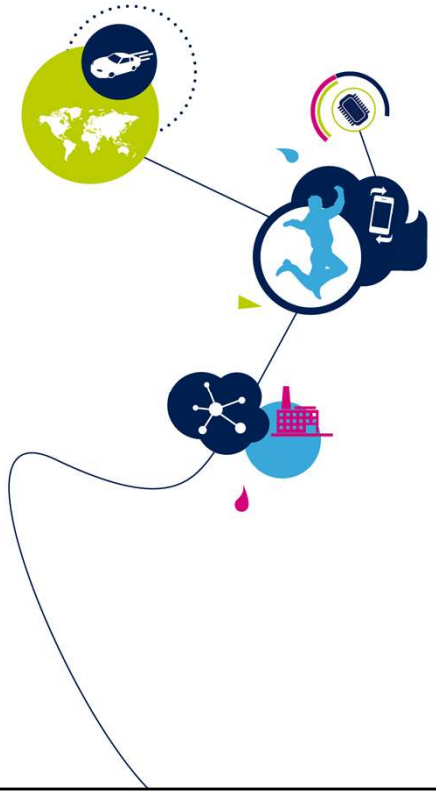
STM32G4 – TAMP

タンパおよびバックアップ·レジスタ

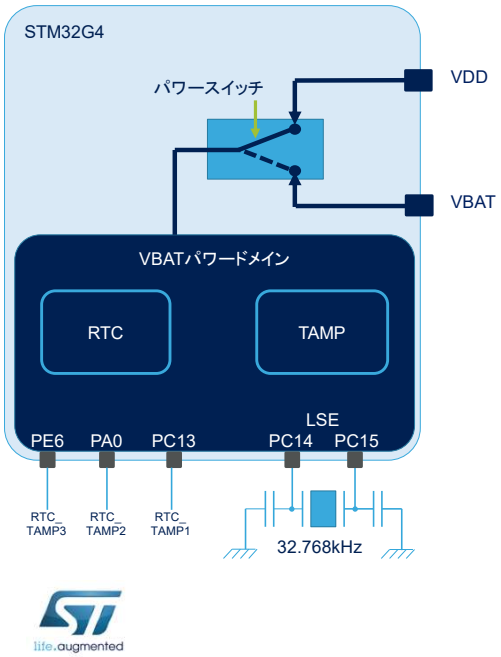
1.0版



life.augmented

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にようこそ。ここでは、改ざんに対するセキュリティを確保するために使用される、このペリフェラルの主な機能について説明します。

概要



- TAMPは32個のバックアップ･レジスタに対してタンパ検出時に消去可能
- 2種類のタンパ入力:外部(3つGPIO)と内部(4つ)
- 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電力タンパ検出

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存するために使用される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(改ざん)イベントが検出されたときに消去されるため、安全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によって供給される場合、タンパ検出は低電力モードで機能します。
改ざん防止回路には、超低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。

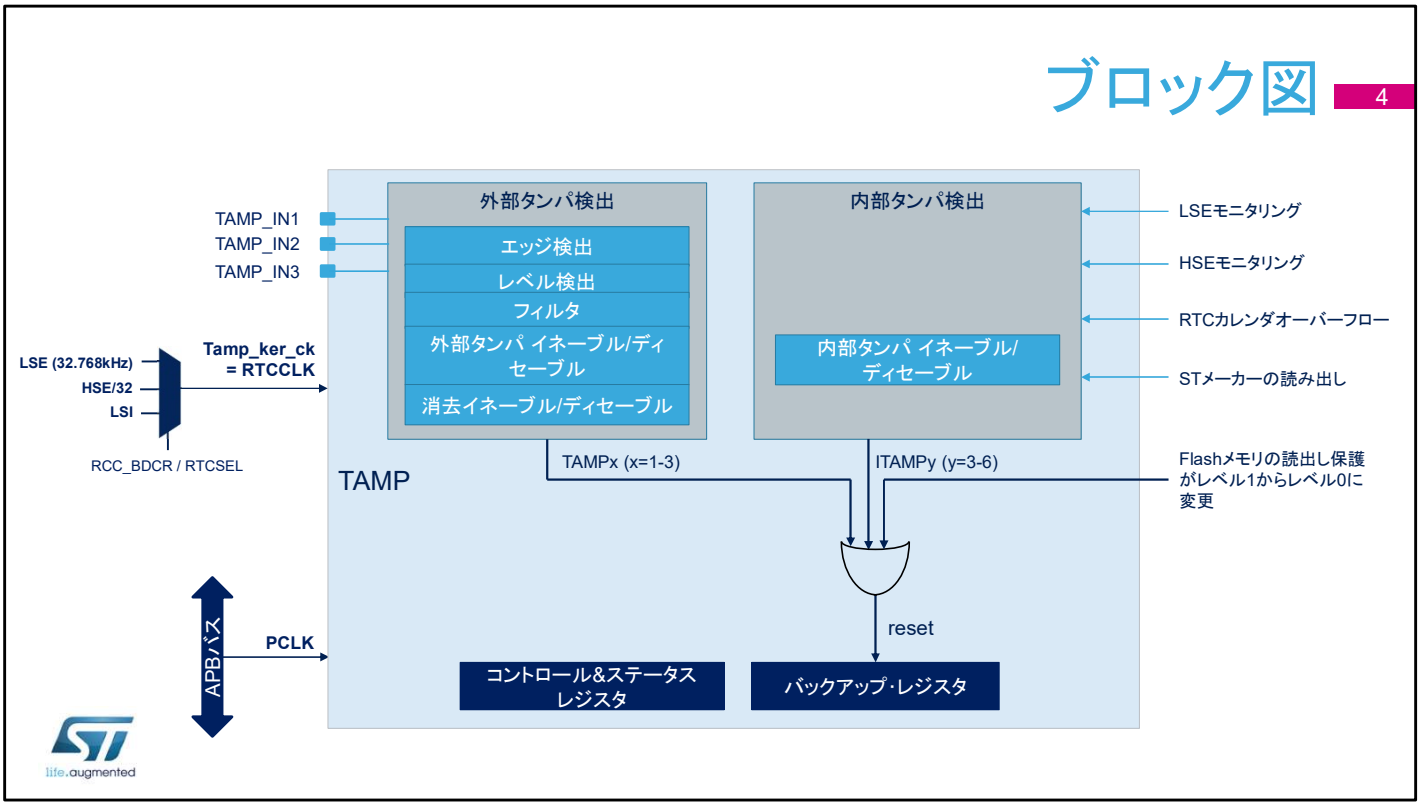
主な機能

- 32個バックアップ·レジスタ:
  - VDD電源がオフの際、VBATによって電源がオンのバッテリ·バックアップ·ドメインにバックアップ·レジスタ(TAMP_BKP0-31R)が実装
- 3個の外部タンパ検出イベント
  - 設定可能なフィルタおよび内部プルアップがある外部のパッシブ·タンパ·イベント
- 4個の内部タンパ·イベント
- タンパ検出は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り、バックアップ·レジスタが消去
  - 外部タンパに関しては、消去を無効にすることも可能

life.augmented

TAMPの主な機能は次のとおりです。
128バイトのバックアップレジスタは、32個の 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、すべての低電力モードおよびVBATモードで保存され、3個のタンパピンのいずれかまたは4個の内部タンパ監視でタンパ検出イベントが発生すると消去されます。外部からの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。
3本のタンパピンはVBATモードで使用できます。
外部タンパイベントは、プログラム可能なエッジ検出、または設定可能なフィルタを使用してレベルで検出することができ、超低電力モードで内部プルアップを使用します。
タイムスタンプ関数は、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。

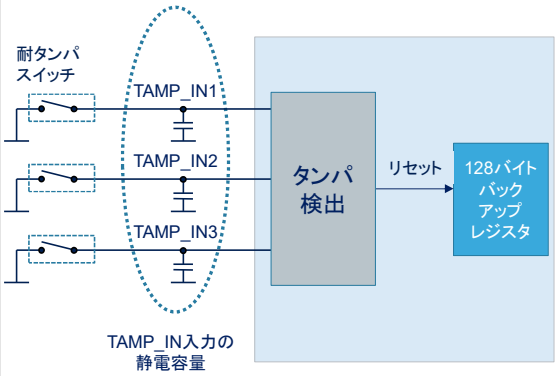
ブロック図



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（または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み取りおよび書き込みアクセスに使用されます。
TAMPクロックは、高速外付けオシレータ（またはHSE）を32で除算、低速外付けオシレータ（またはLSE）、または低速内蔵オシレータ（LSI）のいずれかを使用できます。
LSEまたはLSIのみが、STOPモードとSTANDBYモードで機能します。
SHUTDOWNモードとVBATモードではLSEのみが機能します。
LSEモニタリング、HSEモニタリング、RTCカレンダオーバーフロー、およびSTの読み出しなど、いくつかの内部機能によってタンパイベントが発生する可能性があります。
内部および外部タンパには、それぞれ有効な制御ビットがあります。デフォルトでは、内部タンパは有効になっており、外部タンパは無効になっています。
また既定では、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。外部タンパイベントは、バックアップレジスタを消去しないように設定できます。
バックアップレジスタは、システムのリセットまたはデバイスがSTANDBYモードから復帰したときにリセットされないことに注意してください。
タンパ検出イベントが発生した場合、またはフラッシュの読み出し保護がレベル1からレベル0に変更された場合、バックアップレジスタをリセットできます。

タンパ検出

超低電力耐タンパ回路



- VBATモードで使用できる3個のタンパ入力ピンとイベント
- アクティブエッジまたはレベルでの設定可能
- 外部タンパ・イベントが検出された場合のバックアップ・レジスタのリセット
  - 外部タンパの場合は無効になっている可能性がある
- タンパはタイムスタンプ・イベントを生成可能

life.augmented

タンパの機能は、超低電力のタンパ検出回路を備えています。
その目的は、安全なアプリケーションのために物理的な改ざんを検出し、侵入の場合に機密データを自動的に消去することです。
3個のタンパ入力ピンとイベントがサポートされており、すべての低電力モードや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。
タンパイベントは、侵入の試みの日付を記録するために使用できるタイムスタンプイベントを生成できます。
図に示すコンデンサはフィルタリングを目的としています。
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、配線容量のモデルを気にする必要があります。
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。

タンパ検出

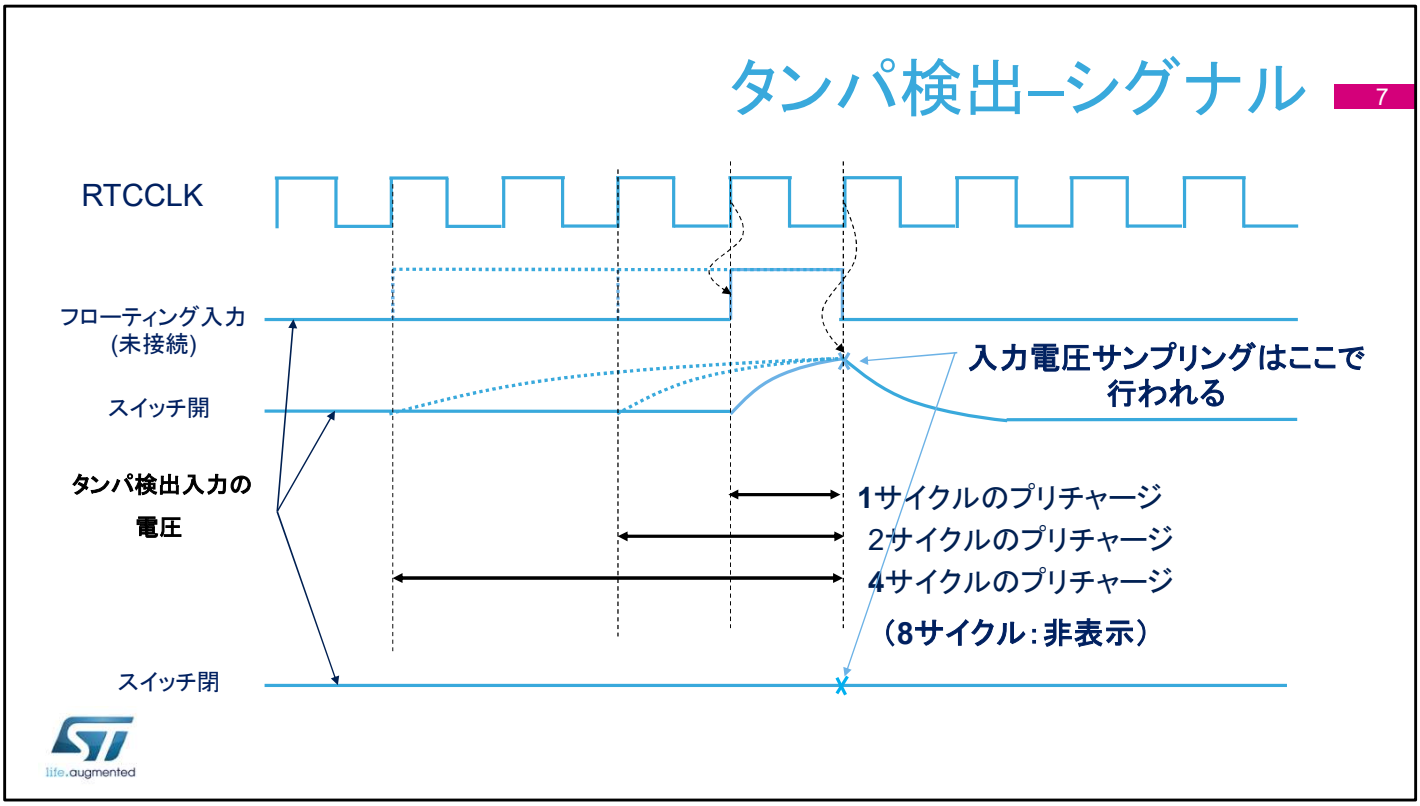
6

フィルタリング付きの安全で超低電力のタンパ検出

- 耐タンパ･スイッチの開状態を検出する設定可能なI/Oプルアップ抵抗の使用
- 異なるコンデンサの値をサポートする設定可能なプリチャージパルス
  - 1、2、4、8サイクル
- 設定可能なフィルタ
  - サンプリング･レート：128、64、32、16、8、4、2、1Hz
  - MCUをウェイクアップさせるための割込みを生成する前の連続する同一のイベント数：1、2、4、8

life.augmented

タンパ検出回路には、超低電力デジタルフィルタが備わっています。
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消費電力を削減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、異なるコンデンサの値をサポートするように設定可能で、1、2、4、8RTC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。
フィルタは、タンパピンに適用できます。
デバイスをウェイクアップさせるための割込みを生成する前に、指定した数の連続する同一のイベントを検出する機能が搭載されています。
この数値は設定可能で、1～128Hz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。



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、レベルはレジスタ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。

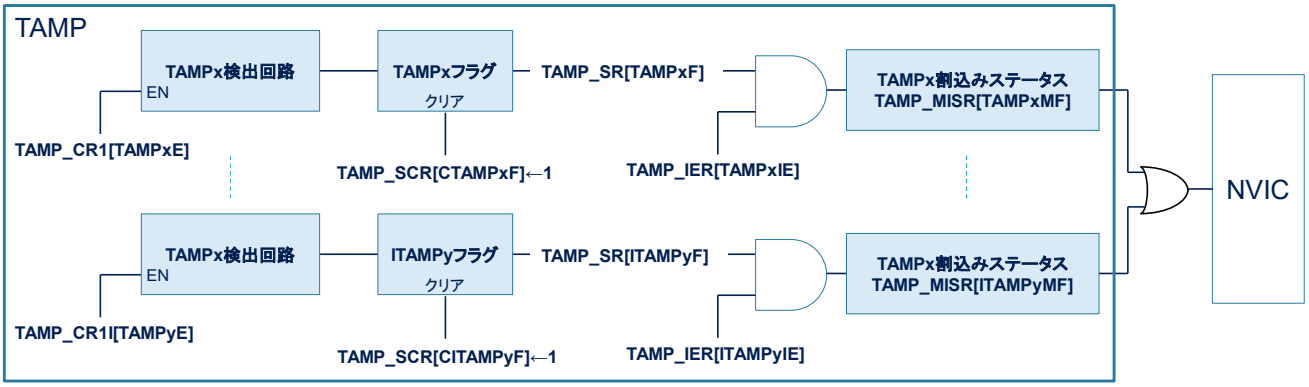
タンパ検出

- 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
  - 各イベントに対して割込みをイネーブル/ディセーブルに出来る
  - 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イネーブルまたはディセーブルにできます。
各外部タンパイベントは、バックアップレジスタを消去するかしないかを個別に構成できます。
各外部タンパイベントは、低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、割込みやトリガ生成のために、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

割込みイベント	説明
TAMPx	TAMP_INxピンで検出されたときにセット
ITAMPy	ITAMP_INy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、すべての低電力モードからプロセッサを起動することができます。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でイネーブルまたはディセーブルにすることができます。
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、対応するフラグがTAMP_SRレジスタに設定されます。
次にTAMP_IERレジスタをマスクするか、タンパイベント割込みを有効にします。
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レジスタを読み取ることによって、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（またはNVIC）には、RTCおよびタンパモジュールに関連する固有の入力があります。

低電力モード

モード	説明
RUN	有効
SLEEP	有効 • TAMP割込みにより、デバイスはSLEEPモードを終了
低電力RUN	有効
低電力SLEEP	有効 • TAMP割込みにより、デバイスは低電力SLEEPモードを終了
STOP0/STOP1	フィルタリングによるレベル検出は、LSEまたはLSIによってクロックされた場合にのみ有効になる • TAMP割込みにより、デバイスはSTOP0/STOP1モードを終了
STANDBY	フィルタリングによるレベル検出は、LSEまたはLSIによってクロックされた場合にのみ有効になる • TAMP割込みにより、デバイスはSTANDBYモードを終了
SHUTDOWN	フィルタリングによるレベル検出は、LSEによってクロックされた場合にのみ有効になる • TAMP割込みにより、デバイスはSHUTDOWNモードを終了

life.augmented

TAMPペリフェラルはすべての低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電力モードを終了します。
STOP0、STOP1、およびSTANDBYモードでは、TAMPのクロックにLSEまたはLSIクロックのみを使用できます。
SHUTDOWNモードではLSEのみが機能します。

関連するペリフェラル

11

- TAMPに関するペリフェラルの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(RTC)
  - リセットおよびクロック制御(RCC)
  - ネスト化されたベクト割込みコントローラ(NVIC)

リアルタイムクロックに関連する周辺機器のリストです。必要に応じて、これらの周辺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
- リセットとクロック制御
- ネスト化されたベクト割込みコントローラ