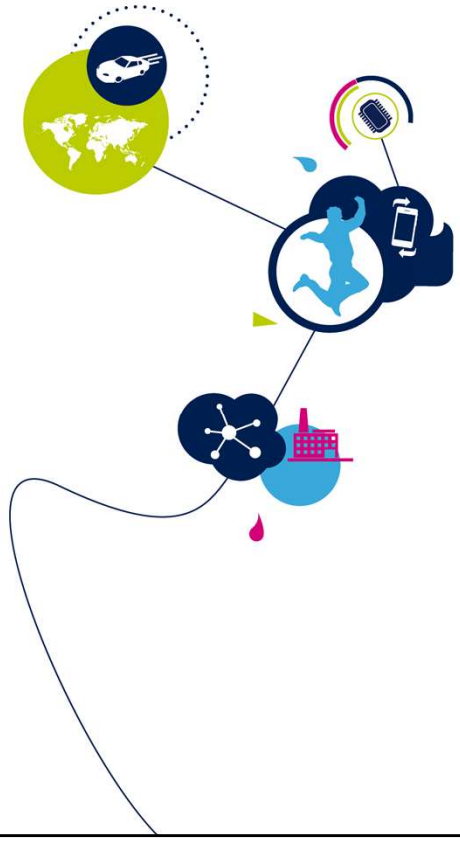
STM32MP1 – TAMP

タンパおよびバックアップレジスタ

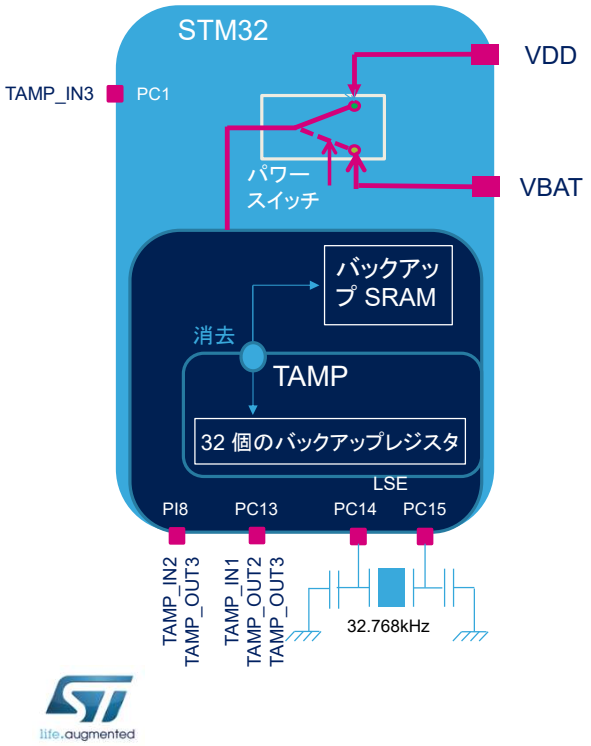
1.0 版



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、物理的および環境的な外部攻撃からの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、3 個の外部タンパイベントと 6 個の内部タンパイベントでの超低電力耐タンパ検出を備えています。
- TrustZone サポートがあります。
- 128バイトのバックアップレジスタおよびバックアップ SRAM があり、タンパ検出時に消去されます。

アプリケーション側の利点

- VBAT での超低電力耐タンパ検出
- オープン短絡外部攻撃からの保護
- 環境的摂動攻撃からの保護

TAMP ペリフェラルは、すべての低電力モードで実行する超低電力耐タンパ検出を備えています。
さらに、主電源がオフになり、VBAT ドメインがバックアップバッテリによって供給されている場合でも、TAMP は機能します。
TAMP ブロックには、主電源がオフのときにデータを保護するために使用される 128バイトのバックアップレジスタが組み込まれています。これらのバックアップレジスタは、タンパピンでタンパイベントが検出されると消去されるため、セキュアデータを格納するために使用できます。また、タンパイベント発生時にはバックアップ SRAM も消去されます。
これらの外部イベントは、セキュリティアプリケーションの要件に応じて 3 種類の設定モードで検出できます。6 個の内部イベントは、組込み監視に基づいて生成でき、環境攻撃からの保護を確保します。
TAMP レジスタは、非セキュアアクセスから保護するために設定できます。

主な機能

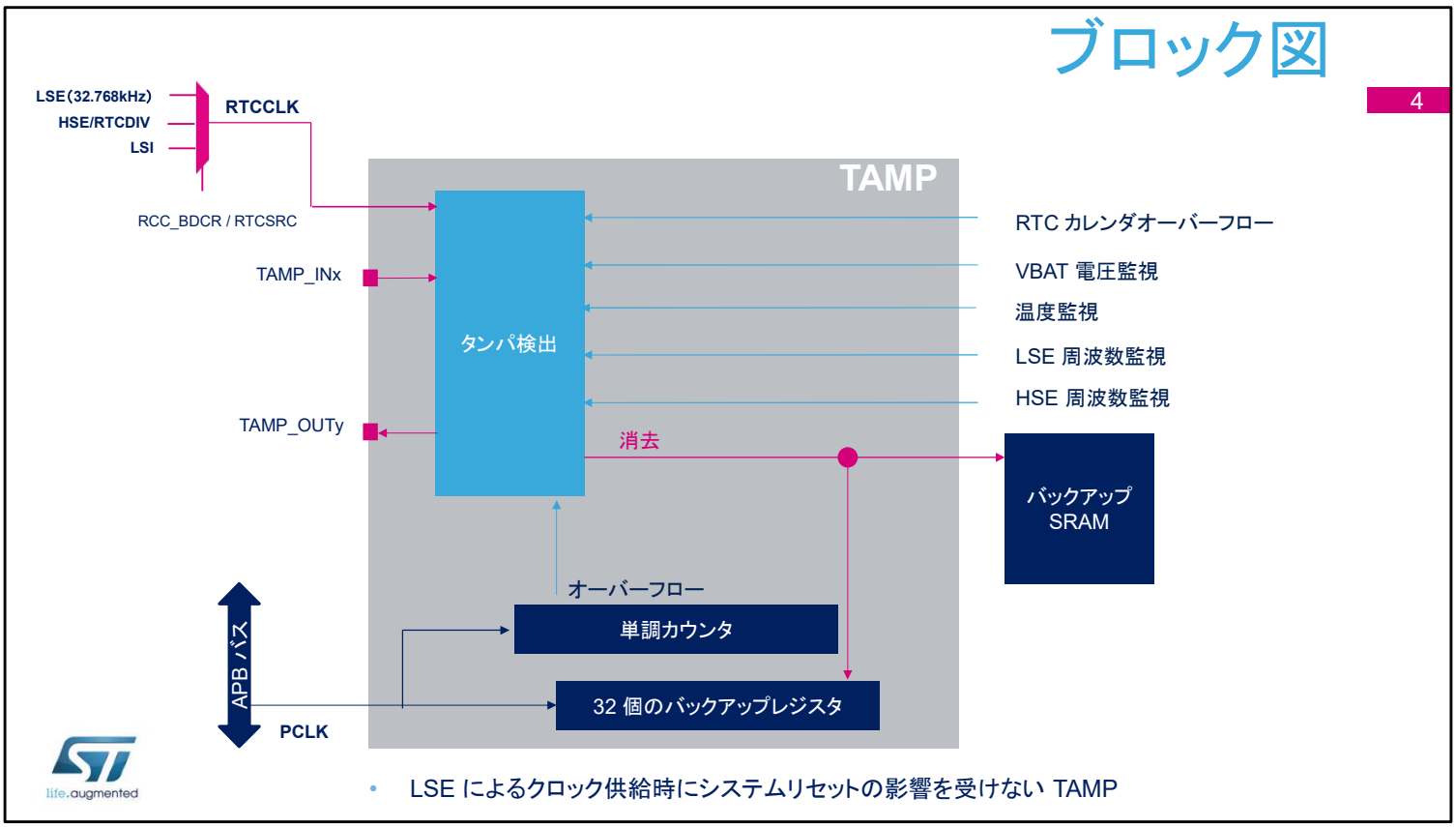
3

- バックアップドメインにある 32 個のバックアップレジスタ（TAMP_BKPxR）
- 3 個の外部タンパ検出イベント
  - VBAT で使用可能な 3 個のパッシブタンパイベントまたは 1 個のアクティブタンパ + 1 個のパッシブイベント
  - デジタルフィルタリング
  - 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
  - 各タンパイベントでバックアップレジスタやバックアップ SRAM を消去するかどうか設定可能
- バックアップレジスタおよびバックアップ SRAM を消去する 6 個の内部タンパイベント
- あらゆる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

life.augmented

TAMP の主な機能は次の通りです。

- 128バイトのバックアップレジスタは、32 個の 32bit 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。
- 最大 3 個の外部タンパイベントがサポートされます。これらのタンパイベントのモードは、パッシブモードまたはアクティブモードに設定でき、すべての低電力モードと VBAT で 3 個のパッシブタンパピンおよびイベント、あるいは 1 個のアクティブタンパ + 1 個のパッシブタンパイベントを使用できます。
- パッシブモードは、I/O エッジ検出または最小電力のタンパ検出モードである設定可能なフィルタリングおよび内部プルアップを備えたレベル検出に設定できます。
- 耐タンパ回路には、超低電力デジタルフィルタが備わっており、I/O での誤ったタンパ検出を回避します。 外部タンパイベントごとに個別にバックアップレジスタやバックアップ SRAM を消去するかどうかを設定できます。
- さまざまな監視による 6 個の内部イベントでも、バックアップレジスタおよびバックアップ SRAM は消去されます。
- タンパイベントによって RTC タイムスタンプイベントを生成できます。



これは、TAMP 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。1 個目はフィルタリングがあるレベルモードでのタンパ検出、およびアクティブタンパ検出にのみ使用される TAMP クロック（RTCCLK）です。
2 個目は、TAMP およびバックアップレジスタの読出しアクセスと書込みアクセスに使用される APB クロックです。タンパエッジ検出や内部タンパ検出にクロックは不要です。TAMP クロックには、リセットおよびクロック制御で RTCDIV 分周回路によって 1～64 分周されるハイスピード外部オシレータ（HSE）を使用できます。その他のクロックソースは、ロースピード外部オシレータ（LSE）かロースピード内部オシレータ（LSI）です。STOP モードおよび STANDBY モードでは、LSE や LSI だけが機能します。VBAT モードでは、LSE だけが機能します。

複数の内部機能によって、温度監視、VBAT 電圧監視、LSE 監視、HSE 監視、RTC カレンダオーバーフロー、単調カウンタオーバーフローといった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でバックアップレジスタおよびバックアップ SRAM が消去されます。

TAMP レジスタ書込み保護

安全な TAMP 初期化

- TAMP レジスタは不正な書込みアクセスを回避するために書込み保護されています。
  - TAMP 書込みアクセスを有効にするには、電力コントローラ制御レジスタ 1（PWR_CR1）でバックアップドメインの無効化（DBP:Disable Backup Domain）ビットをセットする必要があります。

TAMP レジスタはあらゆる不正な書込みアクセスを回避するために書込み保護されています。まず、TAMP 書込みアクセスを有効にするには、電力コントローラ制御レジスタでバックアップドメイン保護の無効化ビットをセットする必要があります。

TAMP セキュリティ保護

TAMP およびバックアップレジスタを保護する柔軟な設定

- バックアップレジスタを除く TAMP レジスタは、TAMP_SMCR レジスタの TAMPDPROT ビットをクリアすることで非セキュア書込みアクセスから全体的に保護できます。TAMP レジスタの読出しはセキュアアクセスや非セキュアアクセスで可能です。
- バックアップレジスタは 3 つの保護ゾーンに分けられ、それぞれのゾーンサイズはレジスタインデックスで設定します。

TAMP は、非セキュア書込みアクセスからの TrustZone 保護をサポートしています。この保護は、TAMP セキュアモード制御レジスタで DECPROT ビットをクリアすることで、バックアップレジスタを除く TAMP レジスタすべてに対してセットできます。DECPROT で保護される TAMP レジスタは、セキュアアクセスおよび非セキュアアクセスで読み出せます。
バックアップレジスタには独自の保護設定があります。
バックアップレジスタは 3 つの保護ゾーンに分けられ、それぞれのゾーンサイズはソフトウェアで設定します。
保護ゾーン 1 は、非セキュア読出しアクセスと非セキュア書込みアクセスから保護されます。このゾーンは、バックアップレジスタ 0 から始まり、TAMP_SMCR レジスタの BKPRWDPROT フィールドで定義されるレジスタまでとなります。
保護ゾーン 2 は、非セキュア書込みアクセスからは保護されますが、セキュアアクセスおよび非セキュアアクセスでの読出しは可能です。このゾーンは、TAMP_SMCR レジスタの BKPRWDPROT フィールドで定義されるレジスタから始まり、TAMP_SMCR レジスタの BKPWDPROT フィールドで定義されるレジスタまでとなります。
保護ゾーン 3 は、非セキュアアクセスから保護されません。このゾーンは、TAMP_SMCR レジスタの BKPWDPROT フィールドで定義されるレジスタから始まり、最後のバックアップレジスタ 31 までとなります。

TAMP セキュリティ保護

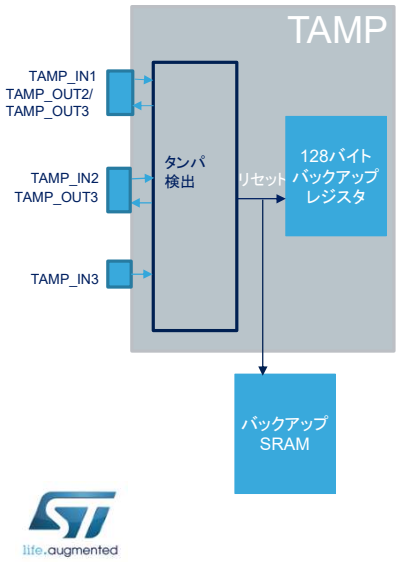
- バックアップドメインのパワーオン・リセット後、セキュアアクセスのみで書込み可能な TAMP セキュアモード制御レジスタ（TAMP_SMCR）を除いて、すべての TAMP レジスタがセキュアアクセスおよび非セキュアアクセスで読出しまたは書込みできます。TAMP 保護設定は、システムリセットの影響を受けません。
- 非セキュアアクセスによる安全に保護されたレジスタへのアクセスは、SILENT モードで実行されます。保護された TAMP レジスタに対する非セキュア読出しでは 0 が返され、保護された TAMP レジスタに対する非セキュア書込みは通知なしで無視されます。
- 1 つ以上の機能がセキュアに設定されると、RTC/TAMP リセットおよびクロック制御も RCC でセキュアになります。

life.augmented

バックアップドメインのパワーオン・リセット後、セキュアアクセスのみで書込み可能な TAMP セキュアモード制御レジスタを除いて、すべての TAMP レジスタがセキュアアクセスおよび非セキュアアクセスで読出しまたは書込みできます。TAMP 保護設定は、システムリセットの影響を受けません。
非セキュアアクセスによる安全に保護されたレジスタへのアクセスは、SILENT モードで実行されます。読出し保護されたレジスタは 0 として読み出され、書込み保護されたビットは通知なしで書き込まれません。
1 つ以上の機能がセキュアに設定されると、RTC および TAMP リセットおよびクロック制御も RCC でセキュアになります。

タンパ検出

超低電力耐タンパ回路

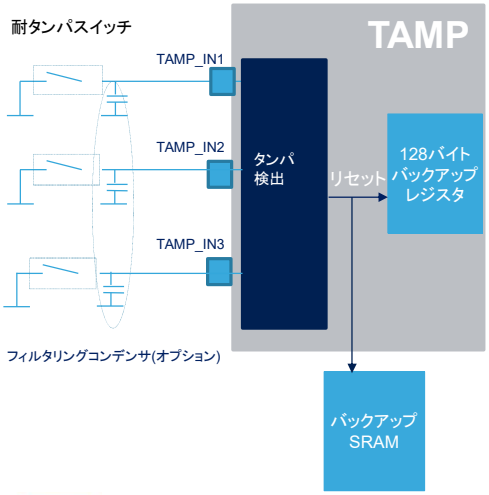


- VBAT モードで使用できる 3 個のタンパ入力ピンとイベント
- VBAT モードで使用できるアクティブモード用の 2 個の出力
- タンパイベント検出時のバックアップレジスタおよびバックアップ SRAM のリセット
  - タンパ検出時にバックアップレジスタおよびバックアップ SRAM をリセットするかどうかは、外部タンパピンソースごとに設定可能です。
  - TAMP_CR2 の BKERASE によって、バックアップレジスタおよびバックアップ SRAM が消去されます。

TAMP 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、外部攻撃からデバイスの内容や機能を保護することです。これはセキュアアプリケーションには必須です。侵入があった場合、機密データが自動的に消去されます。
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。アクティブタンパモードで使用される 2 個の出力ピンは、すべての低電力モードや VBAT モードで機能します。
デフォルト設定では、タンパイベント検出時にバックアップレジスタおよびバックアップ SRAM の内容は消去されます。タンパイベントごとに個別にバックアップレジスタやバックアップ SRAM を消去するかどうかを設定できます。この場合、ソフトウェアがタンパイベントの真偽を識別するためのチェックを実行して、タンパイベントが本物であることが確認された場合に TAMP_CR2 レジスタの BKERASE ビットをセットして、バックアップレジスタおよびバックアップ SRAM の消去開始を判断できます。

パッシブタンパの検出

フィルタリング付きの安全で超低電力のタンパ検出



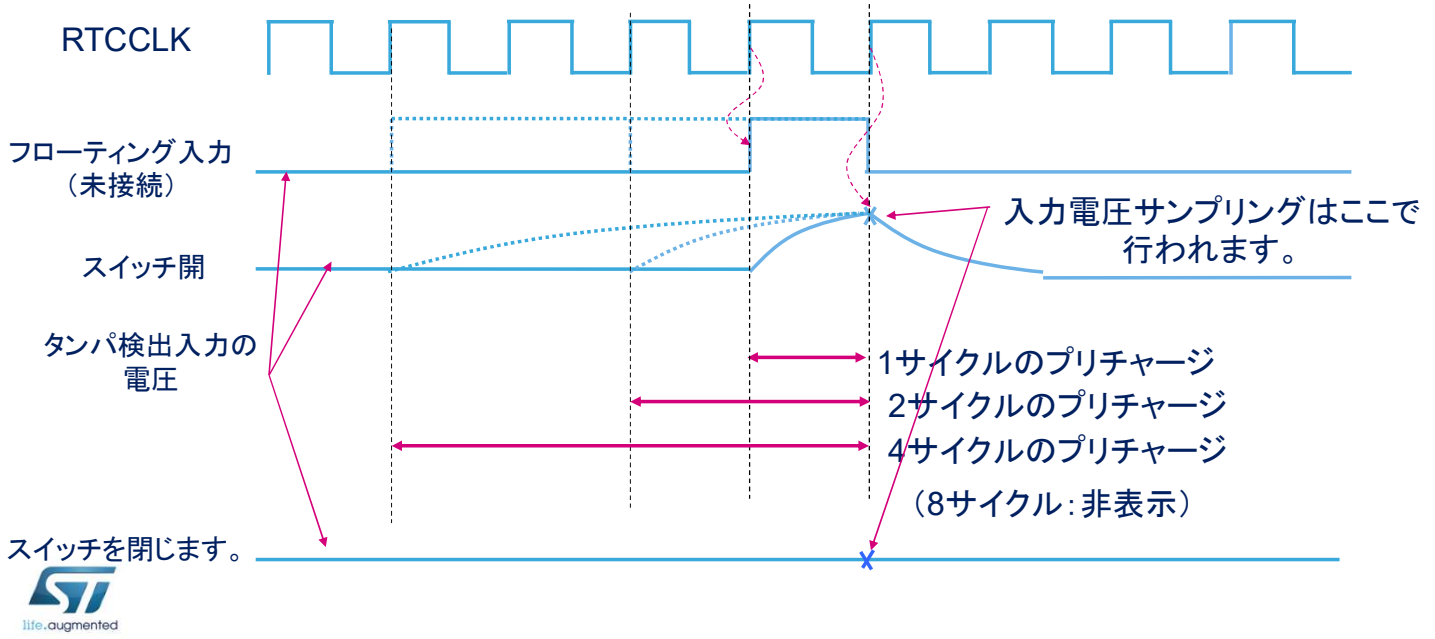
- 2 種類のタンパ検出モード:
  - TAMPFLT = 00:エッジ検出(立ち上がりまたは立ち下がり)
  - TAMPFLT ≠ 00:フィルタリングでのレベル検出
- 耐タンパスイッチの開状態を検出する設定可能な I/O プルアップ抵抗の使用
- 異なるコンデンサの値をサポートする設定可能なプリチャージパルス
  - 1、2、4、8サイクル
- 設定可能なデジタルフィルタ
  - サンプリングレート:128、64、32、16、8、4、2、1Hz
  - MCU をウェイクアップさせるための割込みを生成する前の連続する同一のイベント数:2、4、8

パッシブタンパは、エッジ検出モードまたはフィルタリングモードを備えたレベル検出に設定できます。エッジ検出モードでは、立ち上がりエッジもしくは立ち下がりエッジ検出に設定できます。フィルタリングモードを備えたレベル検出では、内部 I/O プルアップが耐タンパスイッチの開状態の検出に使用されます。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。

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おり、誤ったタンパイベント検出のリスクを低減します。これには、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 2、4、8 個のイベントを設定できます。

パッシブタンパの検出

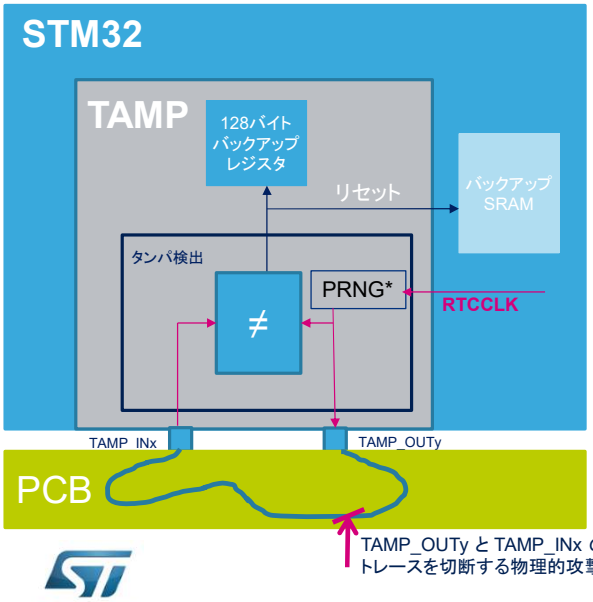
フィルタリング付きの安全で超低電力のタンパ検出



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。

アクティブタンパの検出

最高レベルのセキュリティかつ超低電力のタンパ検出



- 物理的なオープン短絡攻撃を検出する機能でより高度なセキュリティをもたらすアクティブタンパ
  - ランダムパターンが TAMP_OUT ピンで継続的に出力されます。
  - TAMP_OUT は、外部で TAMP_IN ピンに短絡される必要があります。
  - 2 個のピンは継続的に比較されます。
- 設定可能なタンパ検出の最大時間と消費電力
- 柔軟性の高い I/O 管理
  - 各タンパイベントはパッシブまたはアクティブに設定できます。
  - 各入力を任意のタンパ出力と比較できます。
- デジタルフィルタ(オプション)

*:PRNG = 疑似乱数発生器(Pseudo Random Number Generator)

タンパ検出は、セキュリティレベルを高めるためにアクティブモードに設定できます。パッシブタンパの検出は静的レベルをチェックするだけなので、攻撃によってタンパ入力ピンがインアクティブ状態に短絡された場合、タンパイベントが検出されなくなります。アクティブタンパは物理的なオープン短絡攻撃を検出できます。

アクティブタンパを使用すると、MCU が TAMP_OUT ピンで継続的にランダムパターンを出力します。この出力ピンは、外部で TAMP_IN ピンに短絡される必要があります。2 個のピンは継続的に比較され、タンパピンに短絡があった場合や、外部配線が物理的侵入によって破壊された場合に、各 TAMP_OUT 値(乱数発生器より生成)の後に逆の値も送信されるため検出されます。したがって、同じ 0 や 1 の値の長いシーケンスが発生することはありません。TAMP_OUT 値の変更頻度はソフトウェアでプログラム可能で、侵入検出の最大時間に影響します。
TAMP_OUT の頻度を下げて検出時間が増加することで、消費電力を削減できます。
PCB メッシュは、アクティブタンパ検出に使用されます。

タンパイベントは、個別にパッシブ(入力のみ必要)かアクティブ(比較のために出力を入力に関連付ける必要あり)に設定できます。アクティブタンパモードでは、各タンパ入力ピンと比較されるタンパ出力ピンはソフトウェアによって選択され、同じ出力を複数の入力に対して使用できます。

デジタルフィルタは、誤ったタンパイベント検出のリスクを削減するために有効にされます。この場合、連続する 4 つの比較サンプルで 2 つの比較が偽となった場合のみタンパが検出されます。

内部タンパイベント

12

一時的な環境的摂動攻撃からの保護

- 32bit の単調カウンタ、読出し専用、書込みごとにインクリメント、ロールオーバーなし
- バックアップレジスタおよびバックアップ SRAM を消去する 6 個の内部タンパソース
  - ITAMP1：レベルのハイおよびローをプログラム可能な VBAT 電圧監視（PWR のセクションを参照）
  - ITAMP2：レベルのハイおよびローをプログラム可能な温度監視（PWR のセクションを参照）
  - ITAMP3：LSE のトグル停止を検出する LSE クロックセキュリティシステム（LSE CSS：LSE Clock Security System）（RCC のセクションを参照）
  - ITAMP4：HSE のトグル停止を検出する HSE クロックセキュリティシステム（HSE CSS）（RCC のセクションを参照）
  - ITAMP5：RTC カレンダが最大値に達したときに生成される RTC カレンダオーバーフロー
  - ITAMP8：32bit の単調カウンタレジスタ（TAMP_COUNTR）への 2^{32} の書込みの後に生成される単調カウンタオーバーフロー
- 各内部タンパソースの個別の有効化／無効化

life.augmented

環境的摂動攻撃を検出するために、複数の監視がデバイスに組み込まれています。これらの監視は、個別に有効化／無効化できる内部タンパ検出ブロックに接続されており、内部タンパイベントが発生した場合にバックアップレジスタとバックアップ SRAM の内容を消去します。

32bit の単調カウンタが TAMP ペリフェラルに実装されています。このレジスタは読出し専用で、このレジスタに対して書込みアクセスがあると、1 ずつインクリメントされます。このレジスタは、最大値に達するとロールオーバーせずに停止します。このカウンタへの 2 の 32 乗の最後の書込みによってタンパイベントを生成できます。単調カウンタオーバーフローは、内部タンパ検出ブロック 8 に接続されています。

環境的摂動攻撃は、すべての低電力モードおよび VBAT モードで使用できる VBAT 電圧監視と温度監視によって検出できます。各監視のローレベルおよびハイレベルの閾値はプログラム可能です。VBAT 電圧監視は内部タンパ検出ブロック 1 に、温度監視は内部タンパ検出ブロック 2 に接続されています。

RTC クロック攻撃は、LSEのトグル停止を検出するリセットおよびクロック制御の LSE クロックセキュリティシステムによって検出できます。 LSE の CSS はすべての低電力モードで使用できますが、VBAT モードでは使用できません。LSE の CSS は、内部タンパ検出ブロック 3 に接続されています。

HSE がシステムクロックとして使用されている場合、リセットおよびクロック制御の HSE クロックセキュリティシステムによって、HSE のトグル停止時にタンパを生成できます。HSE の CSS は、内部タンパ検出ブロック 4 に接続されています。

RTC カウンタを破損させるソフトウェア攻撃は、RTCカレンダが最大値に達する、99 年 12 月 31 日 23:59:59 に生成される RTC カレンダオーバーフローによって検出できます。このとき、カレンダは停止し、オーバーフローしません。RTC カレンダオーバーフローは、内部タンパ検出ブロック 5 に接続されています。

割込み

割込みイベント	説明
タンパ x(x = 1、2、3)	外部タンパイベントが TAMP_INx ピンで検出されたときにセットされます。
内部タンパ y(y = 1、2、3、4、5、8)	内部タンパイベント y が検出されたときにセットされます。

life.augmented

各タンパ検出イベント(外部および内部)によって割込みを生成できます。

低電力モード

モード	説明
RUN	アクティブです。
SLEEP	アクティブです。
STOP + LP-STOP	アクティブです*。TAMP 割込みによって、デバイスは STOP モードを終了します。 *クロックソースが LSE または LSI である場合のみ、フィルタリングを備えたレベル検出およびアクティブタンパモードはアクティブのままになります。
LPLV-STOP	アクティブです*。TAMP 割込みによって、デバイスは STOP モードを終了します。 *クロックソースが LSE または LSI である場合のみ、フィルタリングを備えたレベル検出およびアクティブタンパモードはアクティブのままになります。
STANDBY	アクティブです*。TAMP 割込みによって、デバイスは STANDBY モードを終了します。 *クロックソースが LSE または LSI である場合のみ、フィルタリングを備えたレベル検出およびアクティブタンパモードはアクティブのままになります。
VBAT	アクティブです*。 *クロックソースが LSE である場合のみ、フィルタリングを備えたレベル検出およびアクティブタンパモードはアクティブのままになります。

life.augmented

TAMP ペリフェラルはすべての低電力モードおよび VBAT モードでアクティブです。STOP モードおよび STANDBY モードで、クロックソースが LSE または LSI である場合のみ、フィルタリングを備えたレベル検出およびアクティブタンパモードはアクティブのままになります。VBAT モードでは、LSE クロックだけが機能することに注意してください。タンパソースが低電力モードで使用できる場合、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。

関連するペリフェラル

- 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。
  - リセットおよびクロック制御（RCC）
  - 電源制御（PWR）
  - リアルタイム・クロック（RTC）

これは、タンパおよびバックアップレジスタペリフェラルに関連するペリフェラルの一覧です。詳細については、必要に応じてこれらのペリフェラルのトレーニングを参照してください。

- リセットおよびクロック制御
- 電源制御
- リアルタイム・クロック