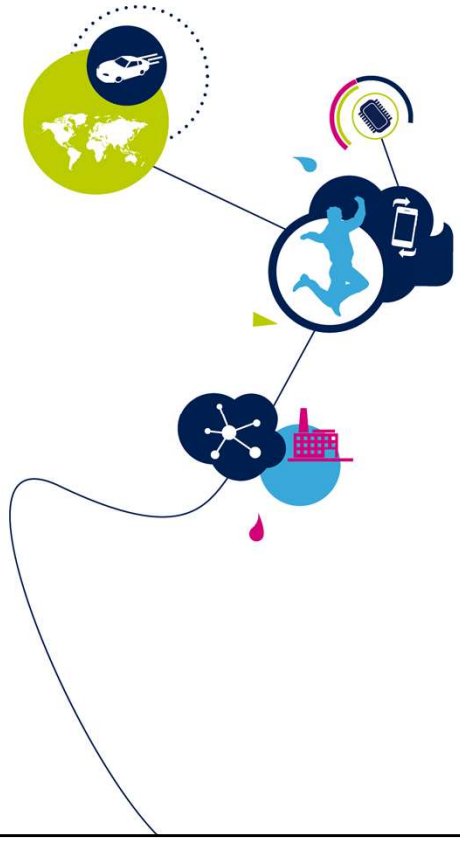
STM32WB - RNG

乱数生成器

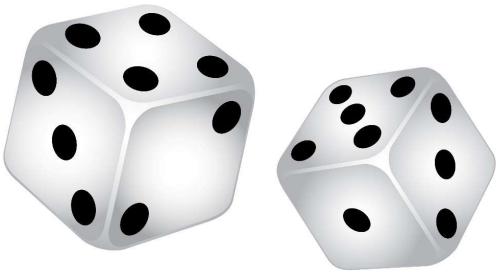
1.0 版



life.augmented

STM32 乱数生成器のプレゼンテーションにようこそ。乱数の提供に広く使用されているこのペリフェラルについて、このプレゼンテーションで説明します。

概要



- 乱数の提供
  - 予測不可能な結果を生み出すことが望まれる場合に使用されます。

アプリケーション側の利点

- 数のランダム性の向上
- 値の推測可能性を著しく減らす

life.augmented

STM32 製品の中に組み込まれている乱数生成器（RNG）は、予測不可能な結果を生み出すことが望まれる場合に使用される乱数を提供します。アプリケーションが RNG から得られる利点は、数のランダム性を上げたり、特定の値の推測可能性を下げたりすることです。

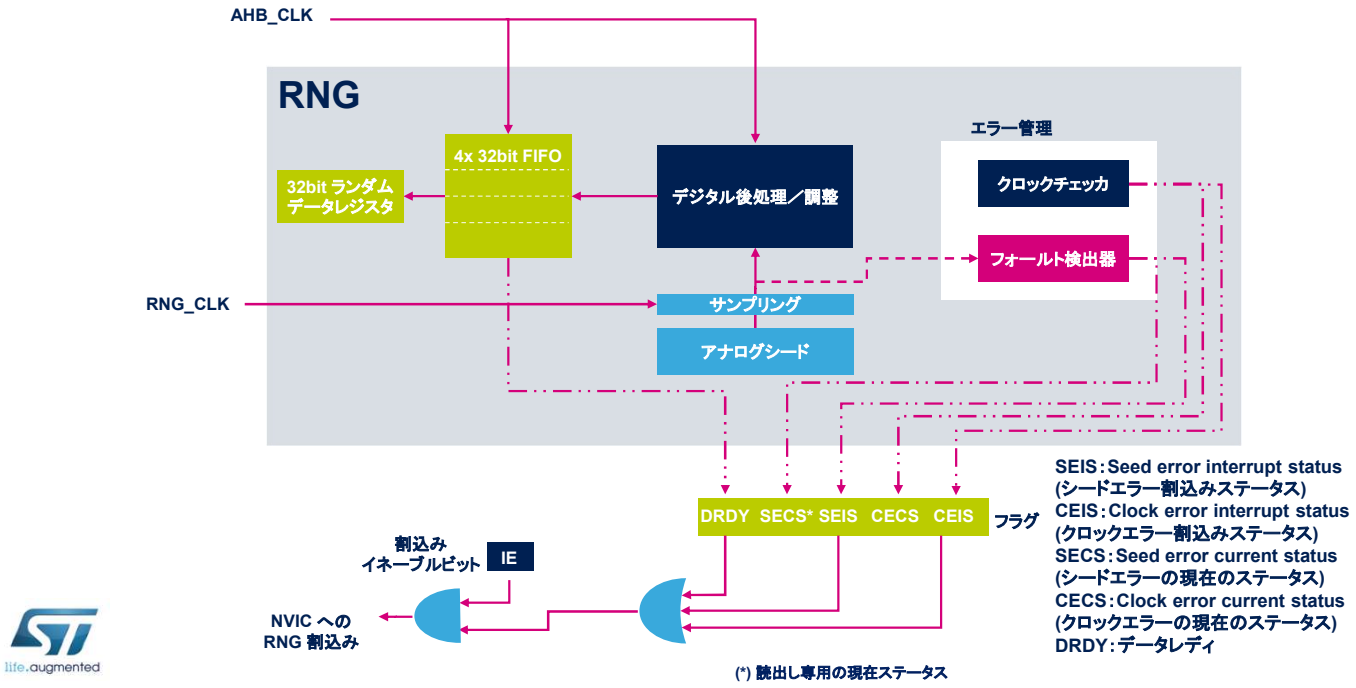
主な機能

- ノイズソースに基づく 32bit乱数生成器
  - 213クロックサイクルの最小周波数で、4 個の 32bit 乱数を生成可能
    - **実際の値（213 よりも大きい場合）は、システムクロックと RNG サンプルクロックの比による 16 x f_{AHB} / f_{RNG} となります。f_{AHB}= 32MHz かつ f_{RNG}= f_{USB} / 3 = 16MHz である場合、サンプルは 213AHB サイクルごとに提供されます。**
  - 本機能を無効にして消費電力を低減することができます（RNG_CR の RNGEN=0）。
- 以下の 3 種類のフラグがトリガ可能
  - DRDY：有効な乱数が準備済み
  - SECS：シードで異常なシーケンスが発生（64bitを超える連続したビットが“0”あるいは“1”の同一値、または“01”あるいは“10”のビットパターンが 32 回を超えて連続）
  - CECS：fRNG 周波数が fAHB / 32 よりも低い（このチェックは無効化可能）
- 3 種類の割込み
  - CEIS：クロックエラーを示します。
  - SEIS：シードエラーを示します。
  - DRDY：有効な乱数が準備済みであることを示します。

life.augmented

RNG ペリフェラルは、連続アナログ雑音に基づいており、詳細は後ほど説明する 32bit の乱数値を返します。RNG は、213システムクロックサイクルの最小周波数で、4 個の 32bit 乱数を生成できます。目安としては、RNG クロックが低いほど、サンプリングされたランダムソースのエントロピーが良くなります。
新しいランダムデータのセットが準備できて検証が終わると、ステータスレジスタのデータレディフラグがセットされます。このフラグは必ず使用する必要があります。
RNG は、提供されたデータのランダム性の基本検証を行います。たとえば、同一の値（0 または 1）が 64bitを超えて連続する場合や、32 回を超えて連続的に 0 と 1 が交互に繰り返される場合には、シードエラーカレントステータスフラグがセットされます。
RNG クロックが 32 で分周された HCLK クロックよりも小さい場合に、クロックエラーカレントステータスフラグがセットされます。
このチェックは、とりわけ、エントロピーを最大とするために RNG クロックが低く初期化された場合に無効にできます。
また、割込みソースを有効にして、異常なシードシーケンスや周波数エラーを示すことができます。

ブロック図



RNG のこの単純化されたブロック図には、その基本的な機能モジュールと制御モジュールが示されています。
乱数生成器は、複数のリングオシレータで構成されるアナログ回路に基づいています。サンプリングされたリングオシレータ出力の排他的論理和をとり、計算ラウンド当たり 4 個の 32bit乱数を生成可能なデジタル後処理ブロックに送り込むシードを生成します。
アナログシードのサンプリングは専用 RNG クロック信号からクロック供給を受けますので、乱数の特性としては HCLK 周波数と無関係になります。後処理ブロックの内容は、4ワードの FIFO を通じてデータレジスタに転送されます。FIFO がフルになるとすぐにデータレディフラグ（DRDY）がトリガされ、それ以上のデータを RNG から読み戻すことができなくなると、自動的にリセットされます。
並行して、エラー管理ブロックにより、正しいシード動作と RNG ソースクロックの周波数が検証されます。
シードの中に異常シーケンスが検出されたり、RNG 周波数が低過ぎたりした場合には、ステータスビットがセットされて割込みがトリガされます。
（品質上の理由などにより）RNG クロックが AHB_CLK/ 32 未満に固定されている場合には、RNG 周波数エラーチェックは無効にする必要があります。

低電力モード

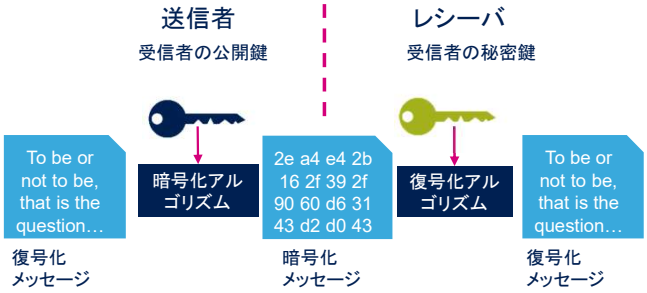
モード	RNG ペリフェラルの説明
RUN	有効
SLEEP	RCC または RNG で無効化されます（RNGEN=0）。RNG を有効に保つと、RNG 初期化時間のためのランダムサンプルが利用可能となるまでのレイテンシが解消されます。
低電力 RUN	消費電力を最小とするために RCC で無効化されます。
低電力 SLEEP	
STOP 0/1/2	
STANDBY	パワーダウン状態です。ペリフェラルは、STANBY モード終了後に再初期化する必要があります。
SHUTDOWN	パワーダウン状態です。ペリフェラルは、SHUTDOWN モード終了後に再初期化する必要があります。

life.augmented

真性乱数生成器は、RUN モードでのみアクティブです。初期化時のレイテンシを回避するために、SLEEP モードで有効に保つことができます。その他の低電力モードでは無効化され、STANDBY モードと SHUTDOWN モードでは完全にパワーダウンされます。

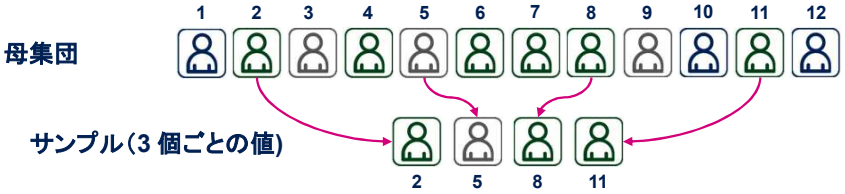
アプリケーション例

- 暗号化



- ゲーム

- 統計的サンプリング



RNG は、暗号、ゲーム、統計的サンプリングを含む幅広いアプリケーションに利用できます。たとえば、暗号化アルゴリズムのすべてのセキュリティは、キーの推測が不可能であることに結び付いています。そのためにキーは乱数である必要があり、そうしないと攻撃者による推測が可能です。

関連ペリフェラル

- RNG に関連したペリフェラル
  - RCC（RNG クロック制御、RNG イネーブル／リセット）
  - 割込み（RNG 割込みマッピング）

これは、乱数生成器に関連した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トレーニングを参照してください。

参照

- AN4230：STM32 microcontrollers random number generation validation using NIST statistical test suite
  - AN4230 は、STM32 マイクロコントローラ群に内蔵されている乱数生成器ペリフェラルによって生成される数のランダム性検証ガイドラインです。この検証は、米国標準技術研究所（NIST）の統計テストスイート（STS）SP 800-22（公開後、2010 年 4 月に SP800-22rev1a として更新）に基づいています。
  - NIST テストスイートは、RNG ペリフェラルを搭載している STM32 ボード群の上で実行されました。 その結果は、ファームウェアフォルダ ‘NIST_Test_Suite_OutputExample’ に格納されています。

詳細については、STM32 MCU 群によって生成される乱数を検証するための NIST 統計テストスイートの使用に関するアプリケーションノート AN4230 を参照してください。