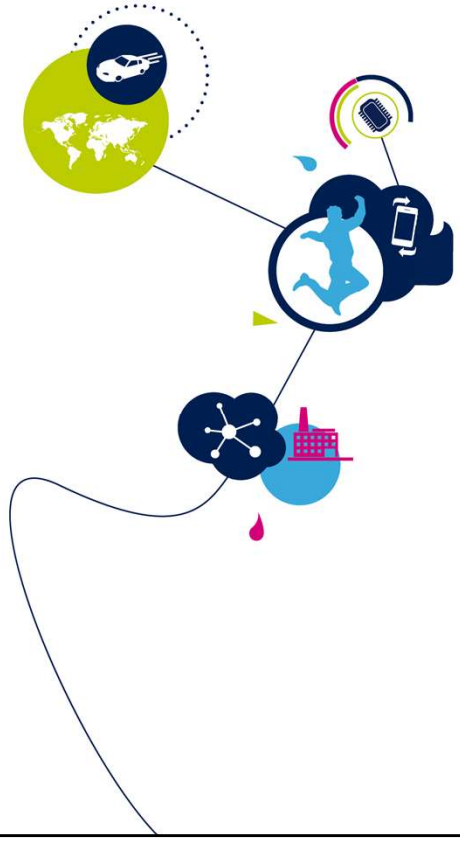
STM32H7 – RNG

真性乱数発生器

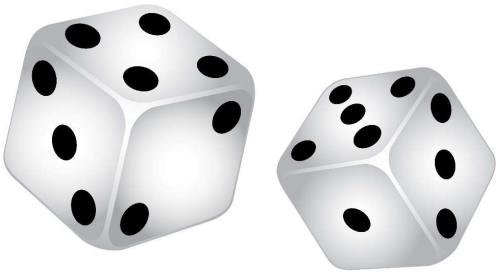
1.0版



life.augmented

STM32乱数発生器のプレゼンテーションにようこそ。このプレゼンテーションでは、乱数の生成に広く使用されている、このペリフェラルの機能について説明します。

概要



- 乱数の生成
  - 予測不可能な結果の生成が求められる場合に使用される

アプリケーション側の利点

- 数字のランダム性を高める
- 値を推測する可能性を低減

STM32製品内に組み込まれた乱数発生器（RNG）は、予測不可能な結果の生成が求められる場合に使用される乱数を生成します。アプリケーションでは、RNGによって数字のランダム性が高まり、特定の値が推測される可能性を下げるというメリットがあります。

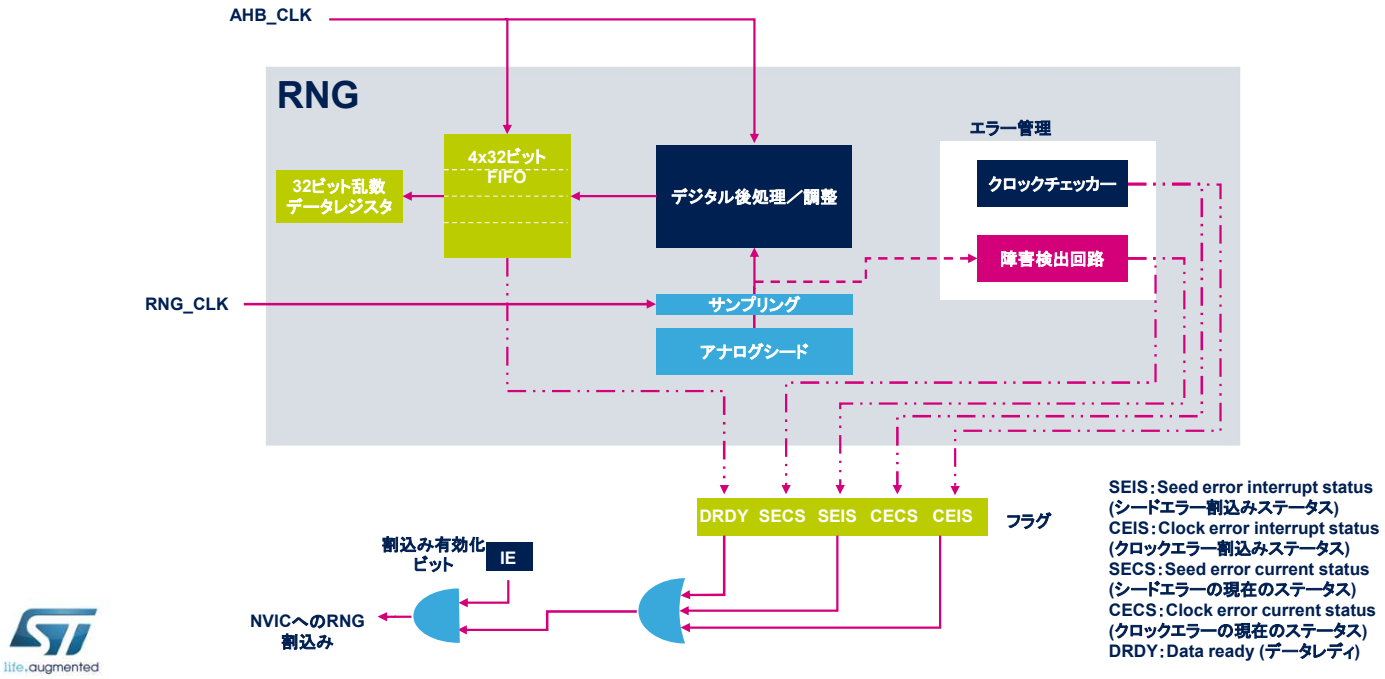
主な機能

- 32ビットの乱数発生器はノイズソースに基づく
  - 4個の32ビット乱数のセットを最低周波数216クロック･サイクルで生成可能
    - 実際の値（216を超えている場合）は32xf_{AHB}/f_{RNG}（システム･クロックとRNGサンプル･クロックの割合）
      STM32H7では、f_{AHB}=216MHzおよびf_{RNG}=f_{CSI}=4MHzの場合、サンプルは864AHBサイクルごとに使用可能
  - 消費電力を低減するために無効にできる
- 次の場合に3つのフラグをトリガ可能
  - DRDY：有効な乱数データが準備できている
  - SECS：シードで異常なシーケンスが発生（64ビット以上連続して“0”や“1”の同じ値、あるいは32ビット以上連続して“01”や“10”のパターン）
  - **CECS**：f_{RNG}周波数がf_{AHB}/32未満（このチェックは無効にできる）
- 3種類の割込み
  - CEIS：クロック･エラーを示す
  - SEIS：シード･エラーを示す
  - DRDY：有効な乱数データが準備できていることを示す

life.augmented

RNGは、後ほど詳細に説明する32ビットの乱数値を生成する連続アナログノイズに基づいています。RNGは、4個の32ビット乱数を最低周波数216システムクロックサイクルで生成できます。おおまかに、RNGクロックが低くなると、サンプリングされる乱数ソースのエントロピーが向上します。
新しい乱数データのセットが準備されて確認されると、データレディフラグがステータスレジスタでセットされます。
RNGは、生成されるデータのランダム性の基本的な検証を実行します。たとえば、64ビット以上連続して同じ値（0や1）である場合や、32ビット以上連続して0と1が入れ替わっている場合、シードエラーの現在の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クロックを下回る場合、クロックエラーの現在のステータスフラグがセットされます。このチェックは、特にRNGクロックがエントロピーを最大化するためにローで初期化される場合に無効にできます。
異常なシードシーケンスや周波数エラーを示すために、割込みソースを有効にすることもできます。

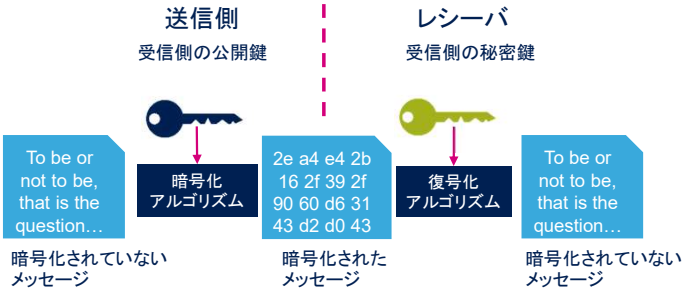
ブロック図



こちらのRNGの簡略化されたブロック図は、基本的な機能モジュールと制御モジュールを示しています。
乱数発生器は、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。その出力は、計算のラウンドごとに4個の32ビット乱数を生成できるデジタル後処理ブロックを供給するシードを生成するためにサンプリングされた後に排他的論理和がとられます。
アナログシードのサンプリングは、専用のRNGクロック信号によってクロック供給されるため、乱数の品質はHCLK周波数から独立しています。後処理ブロックの内容は、4ワードFIFOで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、RNGから読み戻せるデータがなくなると、自動的にリセットされます。
同時に、エラー管理ブロックで、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。
異常なシーケンスがシードで検出された場合や、RNG周波数が低すぎる場合は、ステータスビットがセットされ、割込みがトリガされます。
RNGクロックがAHB_CLK/32を下回って固定されている場合（品質上の理由など）、RNG周波数エラーチェックを無効にする必要があります。

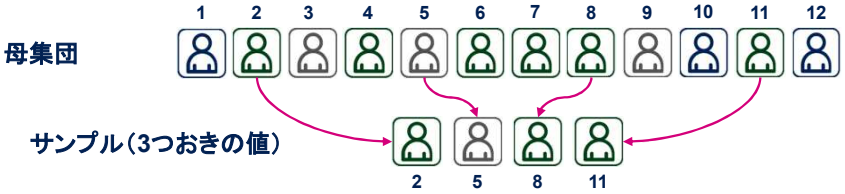
アプリケーション例

- 暗号化



- ゲーム

- 統計サンプリング



RNGは、暗号、ゲーム、統計サンプリングを含む幅広いアプリケーションに使用できます。たとえば、暗号アルゴリズムのセキュリティは、すべて鍵を推測できないようにすることにつながります。そのため、鍵は乱数である必要があり、そうしないと攻撃者が推測できてしまいます。

関連するペリフェラル

- RNGに関連するペリフェラル
  - RCC(RNGクロック･コントロール、RNGイネーブル / リセット)
  - 割込み(RNG割込みマッピング)

life.augmented

これは、乱数発生器に関連するペリフェラルの一覧です。必要に応じて、これらのトレーニングをご参照ください。

参照

- AN4230：STM32 microcontrollers random number generation validation using NIST statistical test suite.
  - AN4230には、STM32マイクロコントローラのセレクションに組み込まれている乱数発生器ペリフェラルによって生成された数字のランダム性を検証するためのガイドラインがある
    この検証は、米国国立標準技術研究所（NIST）の統計テスト・スイート（STS）SP 800-22に基づいており、SP800-22rev1a（2010年4月）として最近発行および更新されている
  - NISTテスト・スイートは、RNGペリフェラルを組み込んだSTM32ボードのセレクションで実行
    その結果は、ファームウェア・フォルダ「NIST_Test_Suite_OutputExample」内にある

詳細については、NIST統計テストスイートに関するアプリケーションノートAN4230を参照して、STM32MCUのセレクションによって生成された乱数を検証ください。